Occupying the Information High Ground:

Chinese Capabilities for Computer Network Operations and Cyber Espionage

Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp

Bryan Krekel
Patton Adams
George Bakos

March 7, 2012

NORTHROP GRUMMAN

Disclaimer:

This research report was prepared at the request of the Commission to support its deliberations. Posting of the Report to the Commission's website is intended to promote greater public understanding of the issues addressed by the Commission in its ongoing assessment of U.S.- China economic relations and their implications for U.S. security, as mandated by Public Law 106-398 and Public Law 108-7. However, it does not necessarily imply an endorsement by the Commission or any individual Commissioner of the views or conclusions expressed in this commissioned research report.

Contents

Acronyms

3G	Third Generation
3PLA	PLA General Staff Department's Third Department
4G	Fourth Generation
4PLA	PLA General Staff Department's Fourth Department
AEW&C	Airborne Early Warning and Control
AMC	Air Mobility Command
AMS	Academy of Military Sciences
AOR	Area of Responsibility
ARMS	Air Refueling Management System
ASIC	Application-Specific Integrated Circuit
BEOL	Back End of Line
BIOS	Basic Input/Output System
BSS	Business Supporting System
BUPT	Beijing University of Posts and Telecommunications
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CATT	China Academy of Telecommunications Technology
CCA	Wuhan Communications Command Academy
CDMA	Code Division Multiple Access
CEME	Complex Electromagnetic Environments
CETC	China Electronic Technology Corporation
CMC	Central Military Commission
CMIPD	Civil-Military Integration Promotion Department
CMOS	Complementary Metal-Oxide Semiconductor
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COCOM	Combatant Command
COMINT	Communications Intelligence
CONUS	Continental United States
COSTIND	Commission of Science, Technology and Industry for National Defense
COTS	Commercial Off-the-Shelf
CVV2	Card Verification Value
DARPA	Defense Advanced Research Projects Agency
DNS	Domain Name Service
DOS	Denial of Service
ECM	Electronic Countermeasures

ELINT	Electronic Intelligence
EW	Electronic Warfare
FEOL	Front End of Line
GAD	General Armaments Department
GLD	General Logistics Department
GPS	Global Positioning System
GSD	General Staff Department
GSM	Global System for Mobile Communications
HIT	The Harbin Institute of Technology
HUMINT	Human Intelligence
IARPA	Intelligence Advanced Research Projects Activity
IC	Integrated Circuit
IDA	Institute for Defense Analyses
IDM	Integrated Device Manufacturer
INEW	Integrated Network Electronic Warfare
IP	Intellectual Property
IRIS	Integrity and Reliability of Integrated System
IT	Information Technology
IW	Information Warfare
JTIDS	Joint Tactical Information Distribution System
LTE	Long Term Evolution
MIIT	Ministry of Industry and Information Technology
MOST	Ministry of Science and Technology
MPS	Ministry of Public Security
MR	Military Region
MSS	Ministry of State Security
NDU	National Defense University
NIPRNET	Non-secure Internet Protocol Router Network
NORINCO	China North Industries Corporation
NUDT	National University of Defense Technology
NWPU	Northwestern Polytechnical University
OFDM	Orthogonal Frequency Division Multiplexing
OPFOR	Opposing Force
OSS	Operation Support System
PACOM	United States Pacific Command
PLA	People's Liberation Army
PLAAF	PLA Air Force
PLAIEU	PLA Information Engineering University
PLAN	PLA Navy
PLANAF	PLA Navy Air Force
PRC	People's Republic of China

R&D	Research and Development
RAM	Random Access Memory
RFID	Radio Frequency Identification
RI	Research Institute
RMA	Revolution in Military Affairs
S&T	Science and Technology
SAR	Synthetic Aperture Radar
SASAC	State-owned Assets Supervision and Administration Commission of the State Council
SASTIND	State Administration of Science, Technology, and Industry for National Defense
SATCOM	Satellite Communications
SIGINT	Signals Intelligence
SOE	State-Owned Enterprise
SQL	Structured Query Language
SS	Diesel Submarine
SSN	Nuclear Submarine
TD-LTE	Time Division-Long Term Evolution
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access
TIC	Trusted Integrated Chips
TPFDL	Time-Phased Force Deployment List
TRANSCOM	United States Transportation Command
TRB	Technical Reconnaissance Bureau
UHF	Ultra-High Frequency
USCC	U.S.-China Economic and Security Review Commission
VPN	Virtual Private Network
WiMAX	Worldwide Interoperability for Microwave Access
ZTE	Zhongxing Telecommunications Corporation

Scope Note

The present study is intended to be a detailed follow up and expansion upon a 2009 assessment prepared for the U.S.-China Economic and Security Review Commission of China's evolving computer network operations capabilities and network intrusion incidents attributed to China. Concern in the United States over alleged Chinese penetrations of both commercial and government networks has only intensified in the past two years as successive incidents have come to light in the media and more organizations voluntarily come forward. The Commission requested a study that both reviewed developments since the 2009 study was completed and examined new issues related to cybersecurity, China, and potential risks to U.S. interests. Specifically, Northrop Grumman information security analysts were tasked by the Commission to address:

1. The state of development in Chinese cyber-warfare strategy including the major military institutions and authors prominent in developing employment concepts and strategic guidance for the People's Liberation Army (PLA);

2. New developments in Chinese practices and capabilities for computer network exploitation to support intelligence penetration and collection against U.S. networks;

3. The potential implications for U.S. military forces in the western Pacific Ocean region, as well as in the continental United States (CONUS) if China staged a network based attack on U.S. systems and infrastructure;

4. The major actors within China (both state-affiliated and state-sponsored) who appear to be engaged in the development computer network operations (CNO) and computer network exploitation (CNE); any identifiable institutional linkages among these groups and government patron organizations supporting them;

5. The activities and research interests of China's most prominent or influential telecommunications research institutes, companies and consortiums and an assessment of any substantive linkages to the PLA, People's Republic of China (PRC) or PRC ministries with security or information technology portfolios;

6. A comparative assessment of the tools and techniques associated with contemporary cyber criminals and with state-sponsored operations originating in China to assess the distinctions that can be drawn in the operations and tools common to cyber criminals and cyber espionage activity;

7. An examination and assessment of the potential network security vulnerabilities, if any, that might be posed by the collaboration between Chinese and U.S. cybersecurity firms.

The Chinese source material for this study came from authoritative PLA publications or authors, PRC government ministries responsible for science and technology policy, Chinese defense industries, China's information technology sector, relevant industry websites and publications, and PRC information technology (IT) industry media and event reporting; additional material related to the role of academia and industry in the development of China's information warfare (IW) programs was obtained from technical journals, research summaries and academic writings sponsored by Chinese universities and PLA and civilian research institutes doing work in IW relevant fields.

Analysis of recent intrusions attributed to China and telecommunications supply chain vulnerabilities are based on non-proprietary, publicly available information. The present analysis of these potential areas of vulnerability is meant to serve as a reference point for continued and more detailed analysis of how U.S. telecommunication supply chains may be better protected in the future.

The result is a comprehensive review of current Chinese efforts to integrate computer network operations into a broader military and intelligence context as well as provide a snapshot of current research and development (R&D) priorities in areas related to CNO. The result will hopefully serve as a useful reference to policymakers, China specialists, and information operations professionals in both industry and government.

Executive Summary

The PLA's sustained modernization effort over the past two decades has driven remarkable transformation within the force and put the creation of modern command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) infrastructure at the heart of the PLA's strategic guidelines for long term development. This priority on C4ISR systems modernization, has in turn been a catalyst for the development of an integrated information warfare (IW) capability capable of defending military and civilian networks while seizing control of an adversary's information systems during a conflict.

Information Warfare Strategy

PLA leaders have embraced the idea that successful warfighting is predicated on the ability to exert control over an adversary's information and information systems, often preemptively. This goal has effectively created a new strategic and tactical high ground, occupying which has become just as important for controlling the battlespace as its geographic equivalent in the physical domain.

The PLA has not publicly disclosed the existence of a computer network operations strategy distinct from other components of IW, such as electronic warfare, psychological operations, kinetic strike, and deception, but rather appears to be working toward the integration of CNO with these components in a unified framework broadly known as "information confrontation." This concept, as discussed by the PLA, seeks to integrate all elements of information warfare—electronic and non-electronic—offensive and defensive under a single command authority.

Earlier in the past decade, the PLA adopted a multi-layered approach to offensive information warfare that it calls Integrated Network Electronic Warfare or INEW strategy. Now, the PLA is moving toward information confrontation as a broader conceptualization that seeks to unite the various components of IW under a single warfare commander. The need to coordinate offensive and defensive missions more closely and ensure these missions are mutually supporting is driven by the recognition that IW must be closely integrated with PLA campaign objectives. The creation of what a probable information assurance command in the General Staff Department bureaucracy suggests that the PLA is possibly creating a more centralized command authority for IW that will possibly be responsible for coordinating at least network defense throughout the PLA.

As Chinese capabilities in joint operations and IW strengthen, the ability to employ them effectively as either deterrence tools or true offensive weapons capable of degrading the military capabilities of technologically advanced nations or hold these nations' critical infrastructure at risk in ways heretofore not possible for China will present U.S. leaders and the leaders of allied nations with a more complex risk calculus when evaluating decisions to

intervene in Chinese initiated conflicts such as aggression against Taiwan or other nations in the Western Pacific region.

Chinese Use of Network Warfare Against the United States

Chinese capabilities in computer network operations have advanced sufficiently to pose genuine risk to U.S. military operations in the event of a conflict. A defense of Taiwan against mainland aggression is the one contingency in the western Pacific Ocean in which success for the United States hinges upon the speed of its response and the ability of the military to arrive on station with sufficient force to defend Taiwan adequately. ***PLA analysts consistently identify logistics and C4ISR infrastructure as U.S. strategic centers of gravity suggesting that PLA commanders will almost certainly attempt to target these system with both electronic countermeasures weapons and network attack and exploitation tools, likely in advance of actual combat to delay U.S. entry or degrade capabilities in a conflict.***

The effects of preemptive penetrations may not be readily observable or detected until after combat has begun or after Chinese computer network attack (CNA) teams have executed their tools against targeted networks. Even if circumstantial evidence points to China as the culprit, no policy currently exists to easily determine appropriate response options to a large scale attack on U.S. military or civilian networks in which definitive attribution is lacking. Beijing, understanding this, may seek to exploit this gray area in U.S. policymaking and legal frameworks to create delays in U.S. command decision making.

Key Entities and Institutions Supporting Chinese Computer Network Operations

The decision to employ computer network operations and INEW capabilities rests with the senior political and military leadership and would be part of a larger issue of employing force during a crisis. Once that decision was made, however, the operational control for the military use of CNO rests with the PLA's Third and Fourth Departments of the General Staff Department (GSD). The Third Department (3PLA), China's primary signals intelligence collector is likely tasked with the network defense and possibly exploitation missions. The Fourth Department (4PLA), the traditional electronic warfare arm of the PLA, likely has the responsibility for conducting network attack missions.

The PRC government actively funds grant programs to support CNO related research in both offensive and defensive in orientation at commercial IT companies and civilian and military universities. A review of PRC university technical programs, curricula, research foci, and funding for research and development in areas contributing to information warfare capabilities illustrates the breadth and complexity of the relationships between the universities, government and military organizations, and commercial high-tech industries countrywide.

In the civilian academic environment, the PRC government (in concert with the PLA in some cases) uses at least five established national grant programs to fund research related to information warfare and to fund the PLA's informationization programs. ***At least 50 civilian universities conducting information security research nationwide benefit from one or more of roughly five main national-level high technology grant programs, reflecting what appears to be a broad technology development plan consistent with published national priorities.***

The PLA is heavily reliant upon China's commercial information technology (IT) sector to aid research and development into dual use and military grade microelectronics and telecommunications. Rather than isolate certain state owned IT firms as exclusively "defense" in orientation, the PLA, often operating through its extensive base of R&D institutes, alternately collaborates with China's civilian IT companies and universities and benefits as a customer of nominally civilian products and R&D. The military benefits because it receives the access to cutting edge research. This work is often carried out by Chinese commercial firms with legitimate foreign partners supplying critical technology and often sharing the cost of the R&D.

A secondary benefit to the PLA of this strategy is the ready access to the latest commercial off-the-shelf (COTS) telecommunications technology brought in by China's access to the foreign joint ventures and international commercial markets.

This close relationship between some of China's—and the world's—largest telecommunications hardware manufacturers creates a potential vector for state sponsored or state directed penetrations of the supply chains for microelectronics supporting U.S. military, civilian government, and high value civilian industry such as defense and telecommunications, though no evidence for such a connection is publicly available.

Potential Risks to the U.S. Telecommunications Supply Chain

The pervasiveness of globally distributed supply chain networks means that virtually every sector of private industry has the potential to be impacted by a compromise. The vectors into the telecommunications and integrated circuit (IC) supply chain specifically can come from either upstream (manufacturing channels) or downstream (distribution channels). Each vector presents distinctive opportunities, and also distinctive operational costs, to potential attackers.

The geographically distributed nature of IC production means that a single chip may incorporate circuits designed in multiple locations around the globe. This model reduces the cost of new product development but it also creates additional security and integrity risks. ***Without strict control of this complex upstream channel, a manufacturer of routers, switches, or other basic telecommunications hardware is exposed to innumerable points of possible tampering and must rely on rigorous and often expensive testing to ensure that the***

semiconductors being delivered are trustworthy and will perform only as specified, with no additional unauthorized capabilities hidden from view.

Deliberate modification of semiconductors upstream of final product assembly and delivery could have subtle or catastrophic effects. An adversary with the capability to gain covert access and monitoring of sensitive systems could degrade a system's mission effectiveness, insert false information or instructions to cause premature failure or complete remote control or destruction of the targeted system. Although the potential for damage can be extreme, the complexity of the technical challenge to alter a design, ensure the compromise is printed on the circuit board, and that the hardware reaches its intended target limits the roster of candidates with the skills and resources necessary to accomplish an upstream supply chain penetration.

A more feasible vector is the downstream distribution channels supplying the targeted organizations where the engineering and logistical challenges are less complex. By providing counterfeit hardware that already contains the Trojanized access built into the firmware or software, a foreign intelligence service or similarly sophisticated attacker has a greater chance of successfully penetrating these downstream supply chains.

The technical and logistical challenges associated with hardware supply chain compromises render these types of attacks generally feasible for only extremely well-resourced organizations, such as nation-state intelligence organizations that have the access to necessary technical personnel to engineer the firmware compromise and the depth of operational expertise to ensure the counterfeit hardware enters the supply chain and reaches its intended target.

Regardless of the sophistication of the attackers, a successful penetration of a telecommunications supply chain such has the potential to cause a catastrophic failure of select systems and networks supporting critical infrastructure for national security or public safety. Although the complexity of these types of attacks may limit the numbers who can succeed, it does not lessen the impact if they do.

A Comparative Analysis of Criminal vs. State Sponsored Network Exploitation

Organized cyber criminals and state-sponsored intelligence professionals conducting computer network exploitation often operate in the same environment and sometimes against similar categories of targets. This overlap poses attribution challenges for information security professionals, policymakers, business leaders, and members of the law enforcement and intelligence communities, all of whom have uniquely different responses to these two groups of actors**.** Distinguishing among them is not merely an academic or theoretical debate. The actions of each group, if left unchecked, have the potential to inflict serious damage to U.S. national security at multiple levels. ***Professional state sponsored intelligence collection not only targets a nation's sensitive national security and policymaking***

information, it increasingly is being used to collect economic and competitive data to aid foreign businesses competing for market share with their U.S. peers.

Media and industry reports portray some of the incidents attributed to China as advanced but the reality is that many successful penetrations are "advanced" only because the targeted organization was unable to stop them or detect the presence of the operators on their networks. Many victim organizations, however, lack the resources to maintain a large or highly skilled information security organizations to adequately defend against these adversaries.

Criminal operations typically do not place value on compromising and maintaining access to a single servers or individual user machines. They require instead high degrees of flexibility and agility to move among many targets within an organization's network.

Activities attributed to state sponsored operators often appear to target data that is not easily monetized in underground criminal online auctions or markets but highly valuable to foreign governments. Highly technical defense engineering information, operational military data, or government policy analysis documents rarely if ever appear to be a priority for cybercriminal groups.

Cyber intelligence analysis must begin considering questions about the likely identity of the end user of stolen information in addition to the identity and affiliation of the attackers to develop insights into what information is likely to be targeted in their organizations. More holistic models that blend counterintelligence analysis and methods with traditional information security engineering are more descriptive and provide greater depth of understanding of the threat in support of information security planning.

Collaboration of U.S. and Chinese Information Security Firms: Risks and Reality

Collaboration between U.S. and Chinese information security firms, while not common to date, has raised concerns over the potential for illicit access to sensitive network vulnerability data at a time when the volume of reporting about Chinese computer network exploitation activities directed against U.S. commercial and government entities remains steady.

To date, the former joint venture between Huawei Shenzhen Technology Company Ltd and Symantec, Inc. is the only major partnering between a Western information security firm and a Chinese high technology company. In November 2011, the partnership announced that after four years of operations, Huawei would buy out Symantec's portion, giving Huawei full ownership of the company. At present, no other information security firms have publicly announced plans for similar deals in China.

The risks arising from future partnerships between U.S. or other Western information security firms and Chinese IT firms are primarily related to the loss of intellectual property and erosion

of long term competitiveness, the same threats faced by many U.S. companies in other sectors entering partnerships in China. Intellectual property theft is a concern for virtually all U.S. businesses operating in China, according to a 2011 survey conducted by the US-China Business Council.

Partnering with an American or other Western anti-virus vendor does not necessarily allow the Chinese partner to obtain signature data earlier than legitimate participation in industry consortia such as the Microsoft Virus Information Alliance, but it may provide the Chinese partner with deeper access to U.S. markets over the long term.

The risks associated with these types of partnerships are not limited to Chinese business partners or to the security industry: these same threats of intellectual property theft exist in numerous industries and countries in which U.S. businesses operate.

Collectively, recent developments in Chinese computer network operations reflect a nation fully engaged in leveraging all available resources to create a diverse, technically advanced ability to operate in cyberspac. ***Computer network operations have assumed a strategic significance for the Chinese leadership that moves beyond solely military applications and is being broadly applied to assist with long term strategies for China's national development.***

Information Warfare: Doctrine, Strategy, and Training

The Chinese People's Liberation Army (PLA) has long considered the ability to seize information dominance as prerequisite for achieving victory in future high tech conflicts, but only recently has it begun to develop the capability to convert this strategic requirement into an operational possibility. Seizing information dominance over an adversary is predicated upon the PLA being able to protect its own networks while disrupting an adversary's information systems. Senior civilian and military leaders alike have identified cyberspace as peer domain of land, air, sea, and space and have charged the PLA with a mission to protect it equally with the others. As a result, PLA planners are developing more comprehensive IW strategies that seek to integrate offensive and defensive missions under a single command entity able to coordinate and deconflict missions while ensuring that these operations support broader campaign objectives in wartime or contribute to the protection of Chinese strategic national interests in peacetime.

China has never issued a formal information warfare strategy document, but it has published high level long term directives, known as the Military Strategic Guidelines *(junshi zhanlue fangzhen* 军事战略方针), that articulate the direction for defense policy and set a long term course for overall military modernization. These guidelines indirectly shape operational art and specific warfighting disciplines such as IW but are not detailed and specific to a single issue area. The Central Military Commission (CMC) has revised the Military Strategic Guidelines only five times since 1949, last in 1993 under Jiang Zemin.[1] The 1993 revisions stated that the PLA should prepare to "fight local wars under high-tech conditions." This guidance was modified at the 16th Party Congress in 2002 when Jiang Zemin stated that the PLA must develop the capability to fight and win "local wars under informationized conditions." Although a seemingly minor change, this language ushered in the PLA's strategic focus on informationization, the ability to link all services and units via shared information systems to sustain and enable joint operations. As a guiding principle of modernization this guidance is helping to drive PLA interest in information warfare broadly and computer network operations more specifically.

The formulation for "Fighting Local Wars Under Informationized Conditions" has set the course for the PLA's strategic transformation through to mid-century and has established a set of milestones to achieve this goal. The first of these milestones was to develop a solid basis for the informationization (*xinxi hua;* 信息化) and mechanization (the application of late 20th century industrial technology to military operations) of the force by 2010, then fully mechanize the force and complete the initial stages of informationization by 2020, achieving complete informationization of the PLA by 2050. Although the plan laid out a clear roadmap for achieving modernization, Chinese military leaders acknowledged that they could not wait to implement this plan in a serial fashion to make the transition to informationization, but had to work three elements of this strategy concurrently. As a result, the CMC decided on a

[1] Hartnett, Dan, "Towards a Globally Focused Chinese Military: The Historic Missions of the Chinese Armed Forces," Center for Naval Analysis, June 2008, CME D0018304.A1, p. 2; OSC ID CPP20080606325001, June 6, 2008.

"leap-ahead development" (*kuayue shi fazhan;* 跨越式发展) approach that put the PLA on a course to continue working for the full mechanization of the force while simultaneously pursuing the development of technologies necessary to achieve the full informationization of the force by 2050. Senior PLA leaders recognized that achieving this goal would require the PLA to integrate its multiple information systems and adopt new models for training, equipping, and operating its forces.

- China's Defense White papers since 2004 have emphasized that the PLA is pursuing "mechanization" and "informationization" concurrently but selectively, opting to work on "leap ahead" capabilities in some areas such as C4ISR and aviation, while upgrading older weapons platforms with a networked capability. This emphasis on C4ISR modernization has been a critical component of the PLA's ongoing transformation.

- The strategy and doctrine changes evident within the PLA since 1999 have largely focused on preparing the military to prosecute short, high intensity campaigns, employ advanced technology to improve combat effectiveness and to be capable of seizing information control. Collectively, these steps were meant to level the technological playing field at the start of combat by concentrating PLA's best capabilities against the enemy's most important assets.[2]

The New Historic Missions

The PRC leadership has reaffirmed this push to long term military modernization repeatedly since the 16th Party Congress in 2002. Under President Hu Jintao's leadership, the PLA promulgated a broad strategic guiding theory during the Party Congress that took "scientific development" as a primary framework for future military modernization planning and expanded the PLA's traditional roles with a new national defense strategy known as the New Historic Missions of the Armed Forces in the New Period of the New Century (*xin shiji xin jieduan wo jun lishi shiming;* 新世纪新阶段我军历史使命).[3] Hu unveiled New Historic Missions, also known as the "Three Provides and the One Role," at an expanded meeting of the CMC in December 2004 shortly after he assumed the chairmanship of the commission and reintroduced it publicly at the 17th Party Congress in 2007. The roles of The New Historic Missions were meant to focus the PLA on developing capabilities that went beyond Taiwan contingencies, and included support to national strategy objectives such as national economic development, expanded territorial interests, and military support to the Communist Party. The New Historic Missions, an outgrowth of Hu Jintao's broader guidance to follow "scientific development" as the leading strategy for military modernization, does not change the PLA's fundamental focus on developing a fully informationized force structure but it does expand

[2] David Finkelstein, "China's National Military Strategy: An Overview Of The "Military Strategic Guidelines" In Roy Kamphausen And Andrew Scobell, Eds, *Right Sizing The People's Liberation Army: Exploring The Contours Of China's Militar*y (U.S. Army Strategic Studies Institute, September 2007): 72.
[3] James. "Chairman Hu and the PLA's 'New Historic Missions,'" *China Leadership Monitor* 27 (Winter 2009).

the scope of PLA responsibilities in significant ways . The New Historic Missions specifically assigned four broad tasks to the PLA that required it to:

1. Provide an assurance for consolidating the party's ruling status;
2. Provide strong security guarantee for ensuring the important strategic opportunity period for national development;
3. Provide a powerful strategic backing for safeguarding national interests;
4. Play an important role in safeguarding world peace and promoting common development."[4]

PLA leaders included additional responsibilities under the third role that identified not only space and distant ocean areas as domains vital to Chinese national security interests, but also included the electromagnetic spectrum—a change that is likely already driving PLA investment in the development of more sophisticated information warfare capabilities.[5] China's increasing reliance on connectivity to international networks for economic activity and the PLA's growing reliance on information systems to support modernization were likely drivers in the decision to identify cyberspace and the electromagnetic domain as areas vital to China's national security.

— The identification of the electromagnetic spectrum as a "fifth domain of the battlespace" places it on equal footing with ground, air, maritime, and space environments.

— A senior researcher at the PLA's Academy of Military Science stated in an interview with the Chinese military publication, *PLA Daily,* that network warfare must be integrated with China's broader national security strategies to support the formation of coherent guidance on cyber defense.[6]

— The capabilities demanded by its expanded roles in the New Historic Missions require the PLA to make significant progress towards its strategic modernization goals, particularly informationization to ensure network connectivity and interoperability among all service branches and units.

[4] Wo Jieming, "Faithfully Carry out the Military's Historic Mission-100 Questions and Answers" (*Zhongshi Luxing Xin Shiji Xin Jieduan Wojun Lishi Shiming Bai Wen Bai Da*") (Changzheng Publishing, 1 May 2006): 1.
[5] "Persist in Taking the Scientific Development as Guidance—Second Commentary on Education Activities on Chinese Military's Loyal Fulfillment of Historic Missions in the New Century and New Stage" (*PLA Daily*, 27 March 2006): 1; Wo Jieming 62.
[6] "Military Experts Share Views on 'Cyber Defense' and National Defense" *PLA Daily,* 6 January 2011.

Informationization and System of Systems Theory

Informationization continues to be the PLA's guiding strategy; to implement it, the PLA has turned to a systems engineering principle called "system of systems operations" (tixi zuo zhan; 体系作战) which they are applying to the integration of information systems as the agent to achieve joint operations goals. These operations guide force-wide training and shape how the PLA approaches tasks such as implementing integrated command networks and joining multiple complex systems across the force.

- The emphasis on system of systems operations is consistent with previously published CMC guidance issued by Hu Jintao and reflects the PLA's perception on the nature of possible future conflicts.[7]

- At a June 2006 all army training conference, Hu declared that "local wars under informationized conditions are confrontations of systems against systems and take the basic form of integrated joint operations."[8]

- The PLA Daily described warfare under informationized conditions as being characterized by opposing sides using complete systems of ground, naval, air, space, and electromagnetic forces.[9]

Definitions of information system-based system of systems theory vary among PLA authors, but most generally focus on using information systems and networks to create a common integrated command infrastructure that links multiple complex "macro-systems" associated with different weapons platforms, C4ISR systems, and units regardless of the domain in which they operate. Information warfare, in the context of systems operations theory, is viewed by some PLA authors as one of many combat macro-systems to be integrated under this concept, but one with the ability to influence battlefield perception, information transmission, and command networks.[10] The systems operations concept fundamentally emphasizes linking all service branches into a common operating picture that can be accessed at multiple echelons of command. System of systems operations are ultimately meant to bring the PLA to a mature joint operations capability.

General Staff Department leaders are planning substantive reforms to PLA training during the 12th Five Year Plan (2011-2015) to accelerate progress toward force integration, according to

[7] Open Source Center, "PRC 2010 Military Training Aims at Strategic Campaigns, Longer Reach" (29 January 2010).
[8] Cao Zhi, "Hu Jintao Emphasizes Importance of Reform and Innovation in Promoting Development of Military Training" (Xinhua Asia-Pacific Service, 27 June 2006).
[9] Li Jinzhong, "Energetically Expand and Deepen Preparations for Military Struggles" (*Dali tazhan he shenhua junshi douzheng zhunbei*) (*PLA Daily*, 7 January 2010).
[10] See as examples: Zhang Hong and Yu Zhao, "Forge New Type of Operational Force Capability System Based on Information System" (*China Military Science,* 2010): 10; LTC Yan Zhensheng, MAJ Liu Haijing, and MAJ Feng Wei, "On Composition And Basic Mode Of Generating Information-System-Based System Of Systems Operational Capabilities" (*China Military Science* 2010): 44; and Li Yanbin, Zhang Ce, and Wu Hongqi, "Information Systems Based System of Systems Operations Command Capability and Study of Its Application" (China Military Science, 2010): 32.

official party and military reporting. System of systems operations principles will form the core of these training reforms underscoring the central role that systems operations plays in PLA training and modernization goals during the 12th Five Year Plan.

- In September 2011, the GSD issued the "Overall Plan for Military Training Reform during the 12th Five Year Program" seeking to establish a new training routine that will enable the PLA to meet the requirements for applying system of systems operations to modern combat.[11]

- The GSD's 2010 and 2011 training directives focused on strategic campaigns (*zhanlue zhanyi),* combined arms objectives, developing proficiency with integrated command platforms, information sharing, and systems operations, according to PLA media outlets.[12]

- The emergence of system of systems operations became a focal point for training in 2010. The 2009 GSD training guidance highlighted the need to conduct system operations under informationized conditions but did not include it as a core theme.[13]

- In 2011, Senior Colonel Wang Xiaoming, deputy director of the All Army Informationization Work Office, one of the PLA's coordinating bodies for implementing informationization modernization efforts among the force structure, published an analysis of system of systems operations that suggests the PLA is still trying to "resolve deep-level contradictions and problems" in the way it approaches the implementation and focus of this construct for information system enhancements.[14]

Information Confrontation Theory

The strategic imperative for the PLA to operate in the electromagnetic domain is driving the formulation of a new approach to information warfare, termed information confrontation (xinxi duikang; 信息对抗), that applies system of systems operations theory to information warfare, viewing it as a macro-system comprised of discrete capabilities linked together under a single command structure and fully integrated into the overall campaign plan. Proponents of the concept note that the application of information confrontation expands

[11] Hu Junhua and Liu Feng'an, "Approved by Chairman Hu and the Central Military Commission: The General Staff Department Promulgates the 'General Plan for Military Training Reform During the '12th Five-Year Program' Period'" (*PLA Daily*, September 23, 2011): 1.
[12] Wu Tianmin, "2010: Military Training of the Three Services To Be Further Promoted" (*PLA Daily*, 8 January 2010): 1; Liu Feng'an. "Chinese Military Exercises in 2010 -- Comprehensively Increasing Core Military Capability." *Junshi Shijie Huakan* (1 December 2010): 46-51.
[13] Wu Dilun et al., "General Staff Department Lays Out Plan for Military Training Throughout the Armed Forces in the New Year" (*PLA Daily*, 7 January 2009).
[14] Wang Xiaoming, "Explorative Study of Laws in Developing Capabilities for Information System-Based System-of-Systems Operations" *China Military Science* 1-2011 (February 2011): 1.

the capabilities of IW to support the war zone commander in a more integrated fashion.[15] Bundling multiple IW capabilities—such as network warfare, electronic warfare, psychological warfare, and underwater acoustic confrontation—into a single coherent system that coordinates offense and defense advances Chinese IW strategy beyond the purely offensive electronic framework of INEW.

- The INEW strategy, which the PLA adopted in 2002, relies on EW to jam, deceive, and suppress the enemy's information acquisition, processing, and dissemination capabilities; CNA, used in conjunction with EW is intended to sabotage information and the networks by which it is transmitted.[16]

- Striking enemy information sensors and networks, sometimes preemptively, to seize information dominance is a core tenet of published PLA campaign strategy, underscoring the role that IW plays in the PLA's overall operational planning.[17]

- A 2008 book, "Informationized Joint Operations" (*Xinxihua Lianhe Zuozhan;* 信息化联合作战), authored by senior PLA officers based in the Nanjing Military Region, identifies network attack and electronic warfare as one of the principal components of future integrated joint operations; and in discussions of "large-sized island joint fire assault operations," specifies the use of CNA to paralyze adversary command and control networks to weaken overall operational effectiveness.[18]

INEW provided the PLA with a coherent model for offensive electronic IW but did not leverage other non-electronic elements such as deception, psychological operations, or kinetic strike, nor did it attempt to link network defense to offensive operations or place them under a single command authority. ***Information confrontation theories currently being developed and refined within the PLA today seek to address these gaps, particularly the need for more coherent command infrastructur***e.[19]

- The 2010 creation of the PLA's Information Assurance Base (*zhongguo renmin jiefangjun xinxi baozhang jidi;* 中国人民解放军信息保障基地), a formal GSD subordinate organization responsible for the coordination and oversight of computer network operations, indicates that the PLA intends to centralize the command of network operations and likely prioritize developing its future defensive and possibly also offensive capabilities. Neither details of this organization's responsibilities nor its

[15] Wang Zhengde, Yang Shisong and Zhou Lin, eds., *Xinxi Duikang Lilun* (Information Confrontation Theory) (PLA Information Engineering University/ Military Science Publishing House, 2007): 124.
[16] Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare" (*Tan Wanglun Yi Tiao Zhan*). *China Military Science* (2002): 112-117.
[17] Peng Guangqiang and Yao Youzhi, eds., *The Science of Military Strategy* (Military Science Publishing House, English Edition, 2005): 338.
[18] Cao Zhangrong, Wu Runbo, and Luo Dong, eds., *Xinxihua Lianhe Zuozhan* (Informationized Joint Operations) (PLA Publishing House, 2008): 2, 63.
[19] Wang Zhengde, Chapter 5; Liu Lifeng, " *Liqing Tixi Zuozhan De Jiben Neihan*" (Clarify Basic Connotations of 'System of Systems' Operations) (*PLA Daily*, 27 January 2011): 10

direct subordination have been made public; however, its position in the GSD bureaucracy suggests that it will have authority over all service branches and possibly the ability to streamline CNO operations.

— The presence of PLA Chief of General Staff General Chen Bingde, four deputy chief of staffs, and the heads of the General Political Department, General Logistics Department and General Armament Department at the unveiling of the new command reflects the likely endorsement it has received from the highest levels of the PLA leadership. Such patronage could translate into bureaucratic authority for the new command to influence the development of computer network operations capabilities across the PLA.[20]

— INEW attacks on an adversary's information systems are not meant to suppress all networks, transmissions, and sensors or to affect their physical destruction, but rather target only those nodes which the PLA's IW planners assess will most deeply affect enemy decisionmaking, operations, and morale. This approach to targeting decisionmaking and seizing information control anticipated the broader framework of information confrontation theory that the PLA is working to adopt.

Operationalizing Information Warfare

The consistent references to aspects of INEW and information confrontation in current PLA IW writings and the focus on integrating these capabilities into field training events suggests that the theoretical debate within the PLA over approaches to IW strategy has largely faded, and the focus has shifted to the integration of IW capable units into the larger force structure. PLA exercises increasingly include network attack, network defense, electronic countermeasures, and psychological operations operating alongside ground, naval, air, and strategic missile forces.

— Chinese media reports on PLA exercises do not explicitly refer to the existence of "INEW units" but they do include frequent reference to field units performing specialized task such as network attack against enemy command networks, electronic countermeasures to disrupt enemy information acquisition, and psychological operations efforts, all components of the PLA's information confrontation theory including the offensive elements of INEW strategy.

— The major PLA named exercises of 2009, 2010, and 2011 have all contained information confrontation focus elements to improve the offensive skills of key units or test the defensive abilities of line units against network and electronic warfare attack.

[20] Peng Pu, "PLA Unveils Nation's First Cyber Center;" Global Times, July 22, 2010, http://military.globaltimes.cn/china/2010-07/554647.html

- Joint-2011 (*Lianhe-211*), a multi-service exercise held in late October 2011 in Shandong Province, included "joint information offensive and defensive operations" as one of the exercise's primary themes, occupying equal prominence with joint fire strikes, joint campaign planning, and joint reconnaissance and early warning, according to the PLA Navy's North Sea Fleet commander quoted on a state-run TV news program.[21]

- "Mission Action 2010,"(*Shiming Xingdong 2010*) a 30,000 troop multi-region exercise held 10 October to 3 November and involving elements of group armies from three military regions, was designed to test the PLA's progress in staging large scale joint operations. The operations featured attacks on participant command and control systems by computer network operations units, according to *PLA Daily* reports, reflecting the continuing strategic priority the leadership places on developing capabilities to seize information superiority by paralyzing enemy information systems.[22]

- GSD Assistant Chief of Staff, Chen Yong, noted in a summary after the exercise that "for the first time, communications and electronic countermeasures as well as network confrontation were carried out throughout the exercise in all stages and all actions, indicating that a new model was created for organizing information system-based system-to-system confrontation drills." [23]

- Leap Forward 2009 (*Kuayue-2009*), a 13 day Guangzhou-based exercise in August 2009 that featured division sized units from three military regions around China, included information confrontation themed missions as one of eight evaluation areas for units participating in the training event. The focus on these skills as a training theme suggests that these capabilities are being integrated with other major mission and functional areas of joint operations.[24]

Despite the PLA leadership's strong endorsement and continued focus on systems operations, information confrontation, and full informationization of the force structure, at least a few senior officers have provided blunt assessments of the shortcomings still being experienced and the apparent contradictions between the Chinese and Western media's portrayal of PLA operational success in these training objectives on one hand and what may be the reality on the ground on the other.

[21] *Military Report* (CCTV-7, 22 October 2011 and 27 October 2011).
[22] "Chinese Military Exercises in 2010 Highlight Five Characteristics" (*PLA Daily*, 21 January 2011).
[23] "Complete Review of 'Mission Action-2010C' Exercise," 10 November 2010, OSC ID CPP20101222478002
[24] "Review of Shenyang MR Efforts for Strengthening Combat Capability Building," 11 November 2009, OSC ID CPP20100417478008

- Chen Weizhan, head of the Military Training and Service Arms Department of the Guangzhou Military Region, according to a September 27, 2011 interview with CCTV-7, said that informationization in the PLA is "still in the beginning phase of overall development, many generations of weapons and equipment exist at the same time, there are considerable gaps in the fundamental conditions of the units, and the level of informationization is not high."[25]

- Most notably, Chen also pointed out the continued existence of "incompatible software systems, unmatched hardware interfaces, and that non-unified data formats are prominent, seriously limiting the execution of the combat unit combined training," and suggesting serious obstacles to the CMC's and General Staff Department's goal of creating a unified and integrated systems operation capability that can provide force-wide common operating pictures at all echelons of command.[26]

[25] "Guangzhou Military Region Article on System-Based Combined Arms Training" (*Zhanshi Bao*, 25 February 2011); *Military Report* (CCTV-7, September 27, 2011).
[26] "Guangzhou Military Region Article on System-Based Combined Arms Training."

The Creation of a Chinese "cyber warfare unit": Guangzhou Military Region's Online Blue Force

The March 2011 disclosure in *Zhanshi Bao*, the official Guangzhou Military Region (MR) Party newspaper, of the creation of an opposition unit for more realistic online training for command staff, elicited widespread speculation in Western and regional media alike that the PLA had created a "super-elite unit of cyberwarriors" designed to carry out network exploitation of foreign networks. According to the *Zhanshi Bao* article, however, the units actually provided network based simulation training for multiple geographically dispersed PLA units across the MR. Rather than network exploitation or other form of INEW mission, the small unit, housed at a Guangzhou training base, said its "main mission [was] to engage combat divisions' headquarters staff participating in…online confrontation exercises involving combat decision-making."

The misidentification of this unit as "cyberwarfare" group resulted from a likely erroneous statement by a PRC Ministry of Defense spokesman during a May 25, 2011 press conference, in which he fused the online nature of the unit's training mission with an offensive cybersecurity role. Media interest in developments and stories concerning Chinese network espionage and attack likely fueled additional mischaracterization and hyperbole in subsequent days.

Blue Force IW Units Enhancing Training Realism

The use of blue force units to enhance training realism has expanded from traditional ground or air opposition forces (OPFOR) to include units with information confrontation missions tasked to create more complicated jamming and network attack environments for participant units in training. The adoption of informationization as a dominant theme in PLA exercises has made the use of "complex electromagnetic environments" (CEME) a standard feature in many training events; however, open source reporting on PLA exercises increasingly notes the specific use of blue force (opposition) units targeting command and control networks via computer network attack or jamming critical communication nodes, suggesting the PLA is focused on preparing units for more realistic information warfare environments and also potentially offering increased training opportunities for those units acting as an OPFOR to gain valuable and more realistic operational experience.

GSD guidance issued in 2006 made the implementation of more realistic live confrontation exercises using blue force units and less scripted training a priority for 2006, according to a *PLA Daily* article, a focus that continues in current operations.[27]

An unidentified artillery regiment In the Chengdu MR developed an INEW-based methodology for a "soft kill" capability that incorporates features such as electromagnetic jamming and computer network attacks into the enemy command and reconnaissance systems, according to a June 2011 article in *Zhanqi Bao*. Most notably, these tools appear to have been developed for integration into the unit's fire support mission, suggesting a model for other non-ECM combat units to incorporate electronic warfare and computer network attack as an organic capability rather than relying solely on dedicated external INEW units for support.[28]

[27] "PLA General Staff Dept Reveal Three Major Military Training Tasks for 2006," PLA Daily, January 3, 2006 OSC ID CPP20060103510001

[28] "Unidentified Yunnan-Based Artillery Regiment Diligently Seeks New Growth Points of Combat Power—Soft Kill Training Included in Plan" (*Zhanqi Bao*, 8 June 2011) 1.

— In Friendship-2010 (*Youyi-2010*), a large-scale multi-MR air defense exercise, blue force ECM units—which possibly included CNA units—conducted a coordinated attack against red force units' information command networks to degrade them, according to an official PLA magazine. These types of evolutions provide some insight into the PLA's ongoing development of tactical applications of INEW on the battlefield and that these tactics are largely consistent with the PLA's campaign strategy for attaining information dominance early in a conflict.[29]

— During Iron-Fist 2009, a large scale multi-MR event described as an "information confrontation exercise" by official Chinese media covering the event, blue force units, referred to as "jamming and information offense-defense units" by official media, successfully suppressed a red force armor and motorized infantry ground assault group's command and control network with a combined network and jamming attack.[30]

— In Mission Action 2010, a multi-MR mobility exercise intended to refine campaign level command of units across MR's down to the regiment level, blue force units combined long range air raids with "electronic jamming and hacker attacks" against red force command and control networks to paralyze operations, according to the Chengdu MR's Party newspaper.[31]

Semi-permanent blue force units appear to be incorporating foreign tactics and command procedures to heighten the realism of their operations, according to a variety of Chinese and official PLA media sources, suggesting that the PLA is serious about developing the capability to defend against the types of attacks the PLA leaders assess they will face from potential adversaries.[32] Several PLA units maintain specialized personnel in dedicated research groups familiar with foreign military tactics and systems to enhance the realism of their training.

– In 2008, a Guangzhou MR electronic countermeasures regiment formed an internal blue team to act as a simulated information combat detachment to develop training methods for the unit to counter various forms of computer network attack. The group reviewed foreign military tactics, employed similar equipment, and consulted unspecified research institutes to upgrade the unit's EW equipment.[33]

[29] Liu Feng'an, "Chinese Military Exercises in 2010," Beijing Military World Pictorial (*Junshi Shijie Huakan)* December 1, 2010 p. 46-51 OSC ID CPP20110310503003

[30] "Iron Fist-2009 Exercise: Red Versus Blue Confrontation of Systems" (CCTV-13, 23 November 2009);

[31] "Majestic and Powerful Forces, Fierce and Sweeping Actions Over a Thousand Miles—Review of, and Thoughts About, the 'Mission Action-2010C' Trans-region Mobile Exercise." *Zhanqi Bao*, 10 November 2010): 1

[32] "Shenyang MR Units Use 'Blue Force' To Strengthen Informatized Operations" (*Qianjin Bao*, 6 May 2008): 1; Jeff Chen and Andrei Chang, "Organization and Combat Capability of PLA Ground Forces" (*Kanwa Asian Defense Review,* September 2007): 20-25.

[33] Luo Ji, Zhang Kejin, "Creating Own 'Blue Army' for the Opposing Force" (*Zhanshi Bao*, 10 March 2008): 1.

PLA Perspectives on Computer Network Exploitation During Peacetime

Authoritative PLA writings on computer network operations typically focus on issues such as the seizure of information dominance during a campaign, shaping adversary perceptions for maximum strategic impact, operating or training under informationized conditions, or strengthening the PLA's network defenses. Discussions of network exploitation and reconnaissance, when they appear, are rarely given the same depth of analysis or discussion as the offensive and defensive capabilities of CNO. Although PLA authors and publications discuss the efficacy of exploiting adversary networks for intelligence gain during wartime, like most countries with mature CNE programs probably do, they avoid acknowledging any active operations.

- One of the most direct authoritative statements on the perceived value of CNE as an intelligence gathering tool comes from authors affiliated with the Academy of Military Science, the PLA's leading institution for doctrine and strategy development. In a June 2011 article in the Communist Party newspaper *Youth Daily* (*Qingnian Bao*), they note that "the quantity of military intelligence information obtained over the Internet is large, the classification level is high, the information is timely, and the cost is low, intelligence reconnaissance activities that are launched over the Internet are already omnipresent and are extremely difficult to defend against."[34]

- In the 2008 PLA book *Informationized Joint Operations* (*Xinxihua Lianhe Zuozhan* 信息化联合作战), which contains an extensive analysis of informationized warfare applied to a "large sized island joint landing operation" Senior Colonel Cao Zhengrong notes that "integrated network electronic reconnaissance" is the foundation and premise of integrated network electronic warfare." However, the book's authors discuss the activity largely in terms of SIGINT oriented collection rather than the exploitation of and access to adversary networks.[35]

Not surprisingly, authoritative Chinese references to the use of network exploitation as a vector for uploading malicious code onto foreign weapons systems or critical infrastructure is extremely sparse; however, a handful of sources make note of the potential value of this type of computer network operation, suggesting that at least some discussion within the PLA has occurred on the subject though operational planning would almost certainly occur within extremely compartmented channels.

- The authors of the PLA published *Information Confrontation Theory* state that information confrontation forces can potentially plant malicious software in enemy weapons systems that will remain dormant until they are employed; or pre-place malware on enemy information systems that will only activate at a preset time to

[34] Ye Zheng and Zhao Baoxian, "How Do You Fight a Network War?" (*Zhongguo Qingnian Bao,* 3 June 2011).
[35] Cao Zhangrong 26-29.

destroy an enemy's C2 network or "those circuits that control operation of railroads and military air routes, or divert trains to wrong routes to cause traffic jams."[36]

[36] Wang Zhengde, Yang Shisong and Zhou Lin, eds. *Xinxi Duikang Lilun* (Information Confrontation Theory) PLA Information Engineering University/ Military Science Publishing House, 2007, p. 12.

Chinese Wartime Use of Computer Network Operations

The following section is a speculative consideration of a Chinese computer network operation against U.S. networks in the context of a possible conflict over Taiwan. While we consider to some extent the possible impact on U.S. forces, this is not a formal net assessment and does not consider in detail possible countermeasures and network defense capabilities that the U.S. military and government may employ that could successfully detect or repel the types of operations described. Details of these defensive capabilities are largely classified. The following does not make any assessment regarding China's intent to conduct any of the scenarios presented.

China has devoted considerable resources toward preparing for potential conflict with technologically advanced nations such as the United States, particularly in the context of a forceful reunification of Taiwan with the mainland. The establishment of The New Historic Missions now requires the PLA to develop capabilities for other contingencies farther from China's littoral waters and for goals more economic than territorial. The bulk of this preparation and military modernization centers on traditional conventional weapons that can target U.S. forces well before they are in range to support Taiwan or otherwise intervene; however, information warfare weapons are increasingly being coordinated with conventional weapons units under the rubric of information confrontation theory in joint-style operations. Countering technologically superior adversaries such as the United States is a longstanding leitmotif of Chinese information warfare writings for the past two decades, but more than simply focusing theoretical discussions, it has deeply informed PLA modernization strategy and doctrinal development.

A defense of Taiwan against mainland occupation is the one contingency in the western Pacific in which success for the United States is dependent upon the speed of response and the ability to arrive on station with sufficient forces to defend Taiwan adequately. Certainly Taiwan is not the only potential flashpoint in the region for which the timeliness of a U.S. response is critical, but it is the one which would likely place the greatest strain on U.S. logistics and command and control infrastructures. Not by coincidence, then, do PLA analysts consistently identify these two components as strategic centers of gravity that potentially both help and hinder U.S. military success in the region.

The general strategic and operational implications of this focus on U.S. logistics and C2 are a staple of analysis in China military studies in the U.S. and elsewhere in the West, [37] but two points bear repeating in the context of Chinese applications of CNO to this problem.

[37] For representative analysis and studies on the PLA anti-access strategies and approaches to countering U.S. military intervention in the Western Pacific, see: Roger Cliff, et al., *Entering the Dragon's Lair: Chinese Anti-Access Strategies and Their Implications for the U.S.,* RAND Corp, 2007; Dean Cheng, *PLA Views of Space: The Prerequisite for Information Dominance,* Center for Naval Analyses, October 2007; and Mark Stokes, *China's Evolving Conventional Strategic Strike Capability* (Project 2049 Institute, 14 September 2009).

First, Chinese offensive network operations targeting the U.S. logistics chain need not focus exclusively on U.S. assets, infrastructure, or territory to create circumstances that could impede U.S. combat effectiveness. PLA strategists are keenly aware that U.S. access to bases in the region face challenges even in the most stable periods. Non-naval forces must rely on a few fixed bases from which to project power into the region during a crisis, access to which is not a guarantee in some cases.[38] Discernible rifts between the U.S. and a given host country could be exacerbated by Chinese network attacks against the host country's infrastructure or military, possibly done overtly to convey the point that the attacks are in response to the host country's support to U.S. forces. Attacks against host country infrastructure that supports U.S. bases or combat operations may be as effective as attempting to penetrate and disrupt U.S. infrastructure or networks in the continental U.S. (CONUS) without risking the potential backlash and escalation of a strike on U.S. soil.

Offensive network operations such as these not only impact physical infrastructure but could expose points of political and diplomatic friction in U.S. relations with the host nation, differences which the Chinese are likely to exploit with the aid of network-based perception and propaganda operations. The ability to create a secondary diplomatic crisis that diverts U.S. leadership attention from the military situation or alters U.S. perceptions of risk conforms to a rich tradition in Chinese IW theory regarding the importance of attacking the enemy cognitively as well as physically and virtually.

Secondly, Chinese strategists and operational leaders view information warfare as a preemptive tool as much as any other element of combat arms. Doctrinal and strategic writings emphasize the importance of seizing information dominance before or at the onset of hostilities and exploiting the use of IW tools for their potential deterrent effect.[39] Computer network attack, in particular, has value for signaling an adversary and underscoring the deterrence message. In a preemptive CNA campaign against U.S. Pacific Command (PACOM) forces, the PLA may start deploying tools via access created in the weeks—or months—prior to any direct U.S.-China conflict. Leveraging what has possibly been nearly a decade of network exploitation work against U.S. military, government and private sector networks, the PLA may target a combination of networks in the PACOM area of responsibility (AOR) that include logistics networks, command and control infrastructure, intelligence collection systems, and potentially civilian targets that directly support military operations such as transportation or other commercial logistics providers. Chinese information warfare strategy emphasizes delaying and paralyzing an enemy's networks in the context of CNO, and even discussions of kinetic strikes are often couched in terms of selecting the appropriate point in the system that will paralyze the overall operation when destroyed.[40] Chinese efforts to defeat the U.S. military in detail and with widespread destructive attack would almost certainly result in an escalation and diversion of their campaign well away from Beijing's

[38] McDevitt, Michael. *China's Naval Modernization: Cause for Storm Warnings?* (The Institute for National Strategic Studies of the National Defense University, 2010): 4.
[39] Peng Guangqiang and Yao Youzhi, eds., 220 and 338; Cao Zhangrong 79, 133-134.
[40] Xie Youlin, "*Zhonggong Tanhuan Zhan Siwei Yu Zhan Li Fazhan Yanxi*" (Study, Analysis of Communist Party of China's Paralysis Warfare, Thought, Combat Force Development) (*National Defense Journal*, 2009): 81.

original strategic intent, and risk forcing Chinese leaders to divert needed resources from a campaign aimed at reunifying Taiwan with the mainland to engage the U.S. in costly and possibly prolonged conflict.

- Military writings on information confrontation and CNO in particular often highlight the deterrent value these tools offer, particularly as a preemptive measure to force the enemy to concede before escalation to full-scale combat.

- One authoritative PLA source notes that deterrence and offense can be conducted simultaneously in information warfare, staging an attack in an effort to induce the adversary to expend valuable resources during a crisis on difficult issues of determining attribution. These writings suggest that these tactics used in coordination can contribute to a PRC bloodless victory using largely information warfare based tools.[41]

As Chinese capabilities and resources for network attack and exploitation continue to improve, PLA commanders will have at their disposal more precise tools that they perceive as offering the ability to be employed on a tactical scale but with the potential for strategic impact on U.S. combat operations or will to fight, without large scale physical destruction or loss of life. When Chinese military planners consider their options for limiting the effectiveness of U.S. intervention during a cross-Strait crisis, the array of available choices is growing rapidly both in breadth and in lethality. Using a vastly improved C4ISR infrastructure—partly a byproduct of the close cooperation between China's commercial IT sector and the PLA—U.S. and allied deployments in the region are likely to be more readily detected and attacked with greater precision than even five years ago.

- Aircraft carrier strike groups operating in the vicinity of Taiwan and beyond are increasingly susceptible to detection by Chinese space-based electronic intelligence (ELINT) satellites, SIGINT collection, and land-based over the horizon radar. The PLA is increasingly able to move data from these collection systems over secure fiber optic cable to commanders at multiple locations and echelons of command thanks to the military's decade of work devoted to informationization.[42]

- The PLA's Second Artillery strategic missile forces have deployed the DF-21D intermediate range anti-ship ballistic missile with a maneuverable warhead equipped with missile defense countermeasures that is capable of targeting U.S. aircraft carrier strike groups up to 1500–2000km from the Chinese coast.[43]

[41] Peng Guangqian, ibid.
[42] Ian Easton and Mark Stokes, "China's Electronic Intelligence (ELINT) Satellite Development" (Project 2049 Institute, 23 February 2011): 14.
[43] Ibid 2.

- Targeting data from other intelligence collection sources, which is itself likely far more refined and precise than was the case even five years ago, can support combined operations among Second Artillery forces, deployed diesel submarines, naval surface combatants with an area air defense capability, and fourth generation maritime strike aircraft.[44]

- The Chinese submarine fleet has improved in both sophistication and quietness with deployment of the new Shang class nuclear fast attack submarine (SSN), the extremely quiet Yuan-class diesel submarine (SS), and the Russian-built Kilo class SS. All of these hulls have the capability for submerged launch anti-ship cruise missile attack, some with ranges in excess of 200nm.[45]

- The PLA Navy Air Force (PLANAF) has continued to refine its maritime strike capabilities and develop proficiency in an air order of battle increasingly composed of fourth generation aircraft such as the Russian Su-30MK2.[46]

- Supporting all of this is a land-, sea-, air-, and space-based integrated C4ISR infrastructure that is vastly more comprehensive than was the case five years ago, and able to provide targeting quality location data on enemy combatants in multiple domains as an integrated common operating picture to many echelons and units.

Computer network operations combined with sophisticated electronic warfare systems are increasingly an option for Chinese commanders as tools improve and more skilled personnel become available to the PLA. To counter sophisticated and multilayered U.S. C4ISR networks, China's defense industries, have devoted resources over the past fifteen years to developing space-based and network-based information warfare capabilities to target U.S. systems in detail.

- Calling space "the ultimate high ground" the PLA has developed credible capabilities for direct ascent kinetic strikes against orbiting satellites, ground-based laser strikes, apparent capabilities for ground-based laser optical countermeasures to imagery satellites. [47]

- Additionally, joint PLA and civilian research into CNE and CNA tools and techniques may provide a more advanced means to penetrate unclassified networks supporting U.S. satellite ground stations.

[44] Stokes, "China's Evolving Conventional Strategic Strike Capability" 1.
[45] U.S. Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Development Regarding the People's Republic of China" (2010): 3.
[46] Ibid 4.
[47] Ibid 30; Mark Stokes and Randall Shriver, *Evolving Capabilities of the People's Liberation Army: Consequences of Coercive Aerospace Power for United States Conventional Deterrence* (Project 2049 Institute, August 2008): 40.

— Computer network attack research and development has focused on stealthier means of deploying tools via more sophisticated rootkits possibly delivering Basic Input/Output System BIOS level exploitation and attack on targeted computer systems.[48]

Chinese commanders may elect to use deep access to critical U.S. networks carrying logistics and command and control data to collect highly valuable real time intelligence or to corrupt, the data without destroying the networks or hardware. Although U.S. network defenses and other countermeasures may call into question the effectiveness of some Chinese tools or approaches to targeting, the PLA's adoption of INEW and information confrontation concepts, which advocate using network operations against C4ISR systems systems, increases the likelihood that they will be a target during a conflict.

- While the PLA has applied the term "paralysis warfare" broadly as an objective for many types of strike missions, INEW style attacks combining CNA and CNE with electronic warfare are uniquely suited to target these types of command and control and logistics systems.[49]

- Unlike traditional air or ballistic missile strikes, network attack and exploitation in particular can be initiated *prior to* the start of traditional hostilities without being a de-facto *cassus belli* and if done properly, can be implemented with little or no attribution back to China.

Chinese writings on CNO and information warfare have long held that enemy command and control, C4ISR, and logistics systems are the primary targets in any conflict against a technologically advanced adversary.[50] ***The consistent identification of U.S. logistics and C4ISR systems as the most important centers of gravity to target in a conflict strongly suggests that PLA commanders will almost certainly attempt to target these system with both electronic countermeasures weapons and network attack and exploitation tools, likely in advance of actual combat or formal U.S. entry into conflict.***

- The 2007 PLA-published book "Informationized Joint Operations*"* (*Xinxihua Lianhe Zuozhan)* asserts that enemy command and control networks and logistics systems will be among the first elements targeted by integrated network electronic forces.[51]

[48]The Basic Input/Output System (BIOS) is a preinstalled program used during startup on IBM PC compatible computers. The CPU initially accesses the BIOS, after which the operating system is loaded.

[49] Xie Youlin, "*Zhonggong Tanhuan Zhan Siwei Yu Zhan Li Fazhan Yanxi*" (Study, Analysis of Communist Party of China's Paralysis Warfare, Thought, Combat Force Development) (*National Defense Journal*, 2009): 83; Nan Li, "The PLA's Evolving Campaign Doctrine and Strategies" in James C. Mulvenon, Richard H. Yang, *The People's Liberation Army in the Information Age* (Rand, 1999): 169.

[50] See for example Cao Zhangrong 79; Dai Qingmin. "Innovating and Developing Views on Information Operations." *China Military Science* (4-2000): 73-77; and Peng Guangqian and Yao Youzhi, eds, *The Science of Military Strategy.*

[51] Cao Zhangrong 79.

- Beginning intensive network operations against U.S. systems prior to actual hostilities would allow operators to either instrument targeted systems or prepare to access previously implanted malicious software for either destructive or passive monitoring missions.

- Chinese planners may attempt to exploit the perceived deterrent value of a widespread preemptive compromise of U.S. military systems by allowing evidence of penetrations to be discovered, suggesting the possibility of much broader compromise with this type of operation.

- Preemptive penetration of PACOM logistics networks in advance of hostilities could create disruptions in information systems or critical infrastructure that could not be easily attributed to Beijing or even perceived as "hacker activity" if they are made to appear as non-malicious system failures.

The effects of preemptive penetrations may not be readily observable or detected until after combat has begun or after Chinese CNA teams have executed their tools against targeted networks. ***Even if circumstantial evidence points to China as the culprit, no legislation or policy currently exists to easily determine appropriate response options to attacks on U.S. military or civilian networks in which definitive attribution is lacking. Beijing, understanding this, could easily exploit such gray areas in U.S. policymaking and legal frameworks to create delays in U.S. command decision making***.

PLA planners and commentators have long assessed that the source of U.S. military effectiveness stems from the ability to integrate military and civilian information systems and leverage this global access to information in combat. Chinese decision makers see this prowess in information technology as both a force multiplier for the United States and a vulnerable center of gravity, calculating that if an adversary is able to disrupt these networks and access information, the effect would leave U.S. combat forces and commanders in a state of paralysis. PLA publications and authors from some of the military's more authoritative institutions have labeled C4ISR systems as "vital point" targets because of this perceived U.S. dependence on the immediate access to information to fight effectively.

- PLA writers affiliated with the Academy of Military Science in a 2011 article in the Academy's primary journal, *China Military Science (Zhongguo Junshi Kexue)* underscored the high return on investment that network paralysis warfare offers when applied to key nodes on the enemy's network, noting that this type of targeting focus makes it possible to achieve an immense operational effect with just a small investment.[52]

- A PLA author writing in an earlier AMS journal article highlighted the value of applying electronic countermeasures and network warfare similar to the INEW strategy to

[52] Ye Zheng and Zhao Baoxian, , "How Do You Fight a Network War?" *Zhongguo Qingnian Bao,* 3 June 2011

target enemy command and control networks, intelligence processing center, communications nodes, power supply; this same author also recommended marshalling network warfare resources from a variety of military and civilian sources to "use virus insertion, deletion of data, and other techniques to paralyze enemy computer networks" (*caiyong zhuru bingdu, shanchu shuju deng cuoshi, tanhuan di jisuanji wangluo;* 采用注入病毒删除数据等措施瘫痪敌计算机网络).[53]

- Researchers at Shanghai Jiao Tong University's Department of Computer Science and Engineering developed a simulation module for "network warfare countermeasures" (*wangluo zhanzheng duikang;* 网络战争对抗) to test high volume denial of service attacks. The system is reportedly capable of generating and sending approximately 14 million network access requests in an unspecified timeframe, according to an unattributed blog posting on a professional developer and information security engineering website,[54] suggesting that focused denial of service attacks are an area of current R&D interest and likely part of the Chinese military CNA repertoire.

To the extent that the PLA and civilian intelligence organizations have been carrying out long term CNE against U.S. networks without retribution or hard evidence of public attribution, Chinese leadership may be emboldened toward greater risk-taking for preemptive network-based attacks or penetrations, potentially increasing the dangers of miscalculation and unintended second and third order effects that lead the United States to escalate the crisis or respond in ways that PLA leaders may not have anticipated.

A Chinese CNO Campaign

PLA information warfare planners and campaign commanders would likely construct a preemptive CNA/CNE strike in a time-phased approach. The operation may begin two or possibly three weeks in advance of overt hostilities to permit sufficient time to gain (or regain) necessary accesses to targeted networks, place data collection tools for intelligence purposes, place malicious payloads for destructive missions and, as the PLA's D-day approaches, to begin modifying databases or corrupting other categories of data to confuse the U.S. command and control picture.

The bulk of effort would likely be directed against PACOM systems in theater and U.S. Transportation Command (TRANSCOM) systems both in theater and in CONUS; however, civilian commercial companies providing direct support or services to TRANSCOM may also be targeted to exploit their trusted network access to military logistics systems.

[53] Cao Shuanze, "*Jituan Jun Jidong Fangwei Zuozhan Xinxi Zhan De Jizhong Zhanfa*" (Information Warfare Tactics in Group Army Mobile Defensive Operations) (*Junshi Xueshu* (Military Art Journal), 1 December 2003): 67.

[54] *Qi Lao Hu Yao Fawei* ("Autumn Tiger"), "*Shanghai Jiao Tong Daxue Jisuanji Xi Kejiu Renyuan Jiufa Wangluo Zhanzheng Duikang Moni Danyuan*" (Shanghai Jiao Tong University Department of Computer Science and Engineering Researchers Develop Network Warfare Countermeasures Simulation Module) (3 September 2011).

- Missions targeting command and control and logistics assets are probably the responsibility of dedicated PLA units with CNE or CNA responsibilities, supported by individuals from civilian organizations including government intelligence ministries, IW militia units with personnel drawn from private sector high tech firms, and elite universities. Given the nebulous relationship between elite freelance hackers and the PRC state security apparatus, it is conceivable that some of these individuals may also be recruited to provide support for selected—but not all—aspects of these operations.

- Initial activity for these units during this two week period would be devoted to verifying access to previously compromised workstations on networks at major U.S. and allied bases around the PACOM AOR in Hawaii, Japan, Guam, Okinawa, and South Korea.

- Teams tasked with targeting U.S. logistics data and networks may begin to implant passive collection tools in compromised NIPRNET nodes and high value civilian contractor networks to capture network traffic related to PACOM's Time-Phased Force Deployment List (TPFDL), the Combatant Command's (COCOM) "blueprint" for the movement of troops and material into theater during a crisis.

- Other CNO teams may be tasked with placing software containing malicious payloads at key network routing nodes; this malicious software might activate automatically at a preselected time or when remotely contacted by one of the CNO teams, and could be coordinated to support other PLA military actions in the overall campaign plan.

- As the date for conflict draws nearer, the PLA may begin more direct offensive action against PACOM and TRANSCOM networks and infrastructure, using existing accesses to target routers for "back rev"[55] or traffic rerouting, or possibly more destructive BIOS level attacks.

Targeting commercial contractors supporting TRANSCOM with sea or airlift for contingency planning could delay the U.S. ability to move personnel and needed supplies into the PACOM theater rapidly. Identifying these companies in advance is possible via open source review of publicly available contracting information. TRANSCOM maintains connections with thousands of external contractor networks, many of which have some level of trusted access to enable civilian contractors to talk to TRANSCOM databases and personnel to maintain functions such as just in time supply and automatic inventory monitoring for aircraft maintenance and general lift planning. Even if TRANSCOM network defenses are well hardened and diligently protected, compromising one of these secondary machines to exploit this trust relationship could provide a "backdoor" into TRANSCOM networks.

[55] Back-revving refers to the returning of system settings or program code to a previous revision that provides known performance. Attackers will back-rev in order to regain access to certain features that may have been removed or rendered inaccessible in newer versions.

- Targeting civilian contractors to TRANSCOM who maintain direct network connectivity for billing, inventory control, and order processing purposes may enable Chinese teams to exploit the logical trust relationships that already exist between these networks and gain access directly to TRANSCOM internal unclassified networks.

- Currently over 90 percent of TRANSCOM's distribution and deployment transactions are handled via unclassified commercial and DoD networks, a factor that has contributed to a 30 percent increase in network penetration attempts against TRANSCOM networks, according to testimony to the Senate Armed Services Committee by the TRANSCOM Combatant Commander, Gen William Fraser.[56]

- If the Chinese CNE team is able to compromise the civilian contractor network via even a rudimentary spearphishing campaign, they will likely attempt to use valid employee network credentials, e.g. certificates, passwords, user names, and most significantly, network permissions, these elements provide all of the same accesses as the legitimate user to immediately begin navigating around the contractor network to compromise other machines and establish a command and control network before attempting to identify high value data or attempt to penetrate TRANSCOM networks directly from the contractor's now compromised system.

- Targeting civilian contractors' system administrators, particularly those with higher level domain level administrator privileges, will give the attackers the ability to create their own accounts at will and assign privileges as they require for their mission; they would in effect have complete control over these critical logistics providers' networks.

- Moving laterally from the civilian company to TRANSCOM networks potentially gives the Chinese teams the ability deploy tools such as network sniffers capable of collecting and transmitting data traversing certain segments of the network. Exploitation teams would likely review this collection for data related to the PACOM TPFDL or similar communications regarding PACOM as a means of providing near-real time intelligence updates on troop and materiel movement.

Chinese operators may have dual missions assigned to them: deploy tools to collect network traffic in support of key intelligence requirements such as PACOM's TPFDL to support Chinese indications and warning intelligence requirements; or a data destruct mission to corrupt commercial or military databases supporting sea and airlift for TRANSCOM prior to the start of a Chinese assault on Taiwan or other military operation. The inability for contractors to access their own systems or data may hinder their ability to respond to TRANSCOM requirements. The Chinese priority on attacking U.S. and allied logistics networks suggests

[56] General William Fraser (USAF), "Testimony, Hearing on U.S. Pacific Command and U.S. Transportation Command in review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program" (Senate Armed Services Committee, 28 February 2012): 40.

that this publicly available information on commercial contractors supporting TRANSCOM is likely a priority collection requirement for PLA planners.

- Exploiting these firms in advance, to possibly create a network of compromised machines in the networks of key contractor who provide strategic lift to TRANSCOM, would greatly streamline CNO missions in the lead up to Chinese combat operations.

- The exploitation of information in contractor databases may support Chinese intelligence requirements related to the deployment orders for specific units or critical supplies as contained in the TPFDL. This data would potentially include details on the date of planned movement, numbers of personnel, tonnage of supplies, dimensions and manifests, destination and the narrow window during which the troops or materiel must arrive at the port of debarkation, all of which allows Chinese commanders to know exactly what units are being deployed, when they arrive, the course or route likely followed, and the nature of the supplies being transported.

- Although valuable for real time intelligence on troop movements, the ability to subsequently corrupt this type of data has the potential to create serious delays in PACOM's ability to move necessary troops and equipment into the theater in time to meet the PACOM commander's mission requirements.

CNO Targeting Case Study

The air refueling mission is one of the most critical daily missions that TRANSCOM provides to U.S. forces around the world. It enables the Air Force to carry out long range global strike missions, extended airborne early warning and control missions (AEW&C), and allows Navy and Air Force fighter aircraft to fly extended combat missions in support of either air superiority or ground attack missions. Most U.S. air combat and combat support missions involve air refueling in some capacity. In the event of a potential cross-Strait crisis that potentially required PACOM combat support to Taiwan, over-water aerial refueling missions would be nearly constant to support both the massive flow of aircraft of all types into the theater and to sustain combat operations once they were there.

TRANSCOM maintains a complex internal management system to coordinate, validate, and deconflict all requests for air refueling support from major combatant commands. This process is managed via TRANSCOM's Air Mobility Command (AMC)[57] which owns the Air Refueling Management System, (ARMS), a web-based application that integrates data from multiple related databases supporting different aspects of the air refueling planning mission. According to TRANSCOM documentation, ARMS is the sole vehicle for all air refueling support requests. Requests for air refueling missions flow into this database, where it is adjudicated based on multiple criteria such as tanker availability, mission priority, and compatibility of receiver aircraft with the tanker. Disrupting the ability to coordinate air refueling has the potential to temporarily ground or delay the movement of fighters, strike aircraft, and valuable heavy airlift into the theater.

- The TRANSCOM Operations and Plans Directorate oversees the Air Refueling Branch which serves as the single focal point within TRANSCOM for all refueling missions management and allows receiver and tanker units to work concurrently with Headquarters AMC's database via the Internet, according to publicly available documentation on the air refueling process.[58]

- Access to ARMS is granted via individual user accounts, according to TRANSCOM documentation,[59] and is likely controlled by a user name and password credentialing and identity management process similar to most access-controlled Internet and Intranet websites. Chinese CNA teams tasked with exploiting or attacking ARMS to impede military air traffic into the PACOM theater would likely start by attempting to identify and target individuals who may already possess a valid ARMS account.

[57] The Air Mobility Command is the air component of TRANSCOM, headquartered at Scott Air Force Base, IL. The AMC fleet can provide refueling capability and deliver people and cargo globally within hours if a crisis warrants. Aircraft assets of the command include: C-17 Globemaster III, C-5 Galaxy, C-141 Starlifter, KC-135 Stratotanker, KC-10 Extender, and C-9 Nightingale. Additional long-range airlift aircraft are available during national emergencies through the Civil Reserve Air Fleet, a fleet of commercial aircraft committed to support the transportation of military forces and material in times of crisis.
[58] U.S. Transportation Command, "Instruction 10-25 Operations: Aerial Refueling" (6 May 2011): 1, 14.
[59] Ibid, 14.

- If these individuals could be identified, Chinese CNE operators would likely begin targeting them with spearphishing emails containing malicious payloads to enable them to upload a keystroke logger on the machine along with malware that allows remote control of the targeted individual's computer to collect ARMS user identification and password data, allowing the PLA team to later log on to ARMS as a legitimate user and possibly create false refueling requests or modify existing records.

- Concurrent with any efforts to target individual ARMS users, Chinese teams would likely beginning scanning this Internet facing application searching for any of thousands of potential vulnerabilities that could be exploited with often longstanding, simple techniques such as structured query language (SQL) injection or cross-site scripting attacks.

- If one of these techniques succeeded, the Chinese operators may begin looking for ARMS records pertaining to air refueling requests in the PACOM theater and begin simply deleting records completely, or attempt to change the air refueling priority codes in these records that determine the operational precedence of the refueling mission, or alter other aspects of the ARMS record such as rendezvous points, and schedules for as many records as possible.

The scenario outlined above is a notional "red team" analysis of an attack against a single potentially high value U.S. military logistics database. PLA commentators have not openly identified specific U.S. networks or databases in their writings about information confrontation, INEW, or related network operations; however, while the operation portrayed here does not take into account potential network defenses surrounding the ARMS or other such databases, it does reflect PLA thinking about the strategic value of targeting adversary logistics systems with the use of CNA tools. This scenario also reflects the PLA's decision making calculus to determine whether to target the data or the network itself in a network attack based on the strategic needs of the PLA larger campaign plan.

An operation such as this notional attack on a TRANSCOM system by skilled Chinese teams would be relatively inexpensive and has the potential for a high return on initial investment of resources and personnel.

- Targeting the civilian contractors to TRANSCOM would not likely be beyond the technical skills for a well resourced Chinese CNA team—be they uniformed military or civilian freelance operators. Relying on an existing toolkit of malicious software perhaps, backed by personnel able to conduct open source research in English and mount systematic targeted email or "spearphishing" campaigns to obtain the necessary user credentials, such a group stands a reasonable chance of successfully bypassing many commercial civilian companies' information security systems.

- A team like this may be compromised of a small group of senior enlisted personnel and junior officers, perhaps most with four year college degrees or technical training

from the military. Alternately, such an operation could be undertaken by skilled IW militia units staffed with information security and IT professionals possessing advanced technical degrees and drawn from high-end Chinese technology firms when their militia units were activated in the weeks prior to the PLA assault.

- The use of purely civilian freelance operators (elite hackers) with an existing relationship with the Chinese Ministry of Public Security (MPS) or Ministry of State Security (MSS) is also a possibility, and anecdotal reporting in the open source suggests that these types of relationships may exist.

- The strategic impact to the United States of this small tactical scale operation would be disproportionately severe relative to effort and resources expended on the Chinese side, achieving a strategic level outcome that Chinese military writings on IW routinely laud as one of the primary benefits of a well planned CNO campaign.

The security of any Internet-facing application is only as strong as the weakest user password, which can negate even the most securely coded application. A professional, well resourced state sponsored team could conceivably target remote users logging into the targeted network from an external location, and capture their login credentials via a man-in-the-middle style attack.[60] Working perhaps well in advance of an actual crisis as part of ongoing, and now routine, peacetime reconnaissance and exploitation operations, teams such as the one described here might successfully establish access to targeted databases or networks such as these.

- The chief executive officer of RSA, one of the world's premier providers of network encryption devices for secure log in and remote access, in October 2011 publicly disclosed his company's assessment that the penetration of RSA networks in early 2011 was a state sponsored operation. This operation resulted in the loss of all information necessary to crack the encryption on any RSA device in use anywhere in the world.[61]

- Defense contractor Lockheed Martin publicly disclosed that a subsequent successful large scale penetration of their network succeeded because the adversary used the data stolen from RSA months earlier to compromise Lockheed Martin employee credentials and gain access to the company's network. Adversaries leveraging the information stolen from RSA succeeded in penetrating an extremely well

[60] A Man-in-the-middle attack, or MITM, is the act of inserting an unauthorized system or process in between trusted communication partners and relaying messages between them. This provides the attacker with the opportunity to intercept and sometimes replace data in transit, unbeknown to either party. MITM attacks are commonly used for data theft, subverting encryption, data insertion to support deception and social engineering.
[61] John Leyden, "RSA Defends Handling Of Two-Pronged SecurId Breach" (*The Register,* 11 October 2011).

instrumented, well protected network staffed by highly skilled information security professionals with a mature cyber intelligence and network defense capability.[62]

While the RSA and Lockheed Martin disclosures stop short of identifying a particular country, they underscore the point that an adversary with the skills and resources to penetrate firms with skilled, dedicated information security professionals and systems may also be capable of penetrating military databases or networks with many connections to non-military commercial systems run by companies lacking the financial resources to maintain these types of multi-layer network security monitoring systems.

Diversionary Attacks

PLA planners may also opt to create additional disruptions intended solely to absorb the time, resources, and attention of the U.S. national leadership, the general public, and media. Such operations could be used to create communications, energy delivery, or other vital services disruptions to the national infrastructure. The attacks need not be debilitating or leave permanent damage but simply cause temporary network or other types of service delivery failures on a localized level but perhaps chosen for likely strategic impact such as in a handful of major urban areas. Chinese government sponsored research into the analysis of U.S. electric grid vulnerabilities has garnered extensive attention in Western media channels because of the suggestion that the PRC government is supporting research intended to identify the vulnerabilities of critical U.S. infrastructure.

- Chinese researchers at Dalian University of Technology, supported by a Ministry of Science and Technology grant administered through the National Natural Science Foundation, published a study on the vulnerabilities of the U.S. power grid to cascade-based attacks. The study found that attacks on nodes with the lowest loads are more effective at creating cascading failures in the Western United States power grid than targeting higher capacity nodes.[63]

- Research on power grid vulnerabilities and prevention of cascading failures is an active field of inquiry among electrical engineers and related disciplines and is not unique to China. This study, however, is unique in its specificity and focus on a named country or region. The Chinese researchers who published this work have specialized in this area and have established publishing credentials in both English language, peer reviewed international journals and Chinese language technical journals, though this is the only study done explicitly on the U.S. system.

[62] Christopher Drew and John Markoff, "Data Breach at Security Firm Linked to Attack on Lockheed Martin" (*New York Times*, 27 May 2011).
[63] Wang Jian-Wei and Li-Li Rong, "Cascade-Based Attack Vulnerability on the U.S. Power Grid" (*Safety Science*, February 2009): 1332-1336.

- This research and another study on attack-induced cascading power failures were sponsored by a grant from the National Natural Science Foundation of China under grant numbers 70571011 and 70771016. The foundation funds an extensive array of research topics including information security and information warfare; however, no open source evidence links these researchers or their work to these formal areas of study.[64]

- The publication of this and related Chinese studies on attack-induced power failures in electrical grids in international English language technical journals suggests that the work was not sensitive to the PRC or likely in support of sensitive CNA programs. An alternative scenario, however, might be some PRC intention to signal its interest in the subject, particularly U.S. networks. This is highly speculative, however, and lacks evidence in the open source.

PLA strategic and doctrinal writings on information confrontation stress the importance of attacking or shaping the adversary's perceptions, sometimes via the networks or systems themselves with false or corrupted data during a conflict or crisis.[65] CNA operations against U.S. infrastructure during the weeks leading up to the initiation of a military campaign against Taiwan may support a broader campaign to shape U.S. leaders' perceptions of the nature of the crisis they must manage. Network attacks to create multiple large scale network or power grid failures, seemingly unrelated to rising tensions with China, may force a U.S. president and his national security team to divert time or resources to manage the domestic emergency. Electric grid outages in densely populated areas of the United States or attacks against networks supporting financial institutions could put significant strain on U.S. policymakers to coordinate domestic crisis management, and while simultaneously attempting to deal with impending or actual hostilities in the Taiwan Strait.

In addition to targeting localized portions of the electrical grid to create periodic blackouts leading up to the PLA's D-day, Chinese operators may employ deceptive CNE and CNA missions against portions of the U.S. Government that are, in effect, nuisance attacks designed to absorb agency resources or degrade communications as the national security leadership attempts to coordinate a response to rising tensions with China.

- The attacks could be basic and "noisy" such as destructive attacks on network mail servers at the State Department, Transportation Department, or Treasury Department. Mail and messaging servers (such as Microsoft Exchange) process email

[64] Wang Jian-Wei and Li-Li Rong, "Edge-based Attack induced Cascading Failures On Scale-Free Networks" (*Physica A: Journal of Statistical Mechanics and its Applications*, 2009): 1731-1737.

[65] Wang Zhengde, Yang Shisong and Zhou Lin, eds., *Xinxi Duikang Lilun* (Information Confrontation Theory) (PLA Information Engineering University/ Military Science Publishing House, 2007): 251+; Peng Guangqiang and Yao Youzhi, eds.: 374; Pan Chin-chang, "*Lun Gong Jun Zixun Hua Zhanzheng Zhi Xinli Zhan*" (On the Role of Psychological Warfare as a Part of the PLA's Informatized Warfare Operations) (Army Studies Bimonthly, April 2007): 18-19; Yang Baoming, Zhao Changjun, and Xu Jianhua, "Dialectical Considerations On Operation Guidance Under Informatized Conditions" (China Military Science, 2010): 73-83.

transactions on a network and losing even portions of their functionality at the height of a crisis could delay communications, when the need for rapid inter-agency coordination and crisis management is at a peak.

- Brute force attacks such as these may be intentionally "noisy" to attract attention and consume resources with the intent to distract network security specialists away from other more substantive, and subtle, CNO activities elsewhere. A series of these kinds of operations, noisy and public but difficult to attribute to China definitively, may increase the "fog" obscuring policymakers' abilities to obtain clear information about an imminent or ongoing crisis, perhaps just as China begins its assault across the Strait.

The decision to move beyond strictly military targets for network attack operations would likely be made at the highest levels of China's military and political leadership because of the recognized dangers of escalation that such a move presents. Targeting elements of U.S. infrastructure that support financial markets means that sudden disruptions to the clearing and settlement infrastructure (even if only experienced by one participant in a geographically limited area) can quickly cascade into market-wide liquidity dislocations, solvency problems, and severe operational inefficiencies, according to U.S. Federal Reserve analysis.[66]

- These effects were widely observed in the days following the September 11, 2001 terrorist attacks, and financial industry regulators and industry members initiated an extensive top-down review of lessons learned; this study codified a detailed best practices list to contain a similar disruption.[67]

- The majority of the clearance and settlement infrastructure has become concentrated in the U.S. over the past three decades, potentially magnifying the international effects of an attack against U.S.-based financial systems.

As the Chinese D-day draws closer, more direct offensive measures may be employed, possibly using tools that were pre-deployed via earlier CNE penetrations. CNE tools with BIOS destruct payloads emplaced on PACOM and TRANSCOM computers with an activation that is timed to correspond to other movements or phases of a larger Chinese campaign plan could create catastrophic hardware failures in key networks. CNE efforts against PACOM networks to understand the network topology and command relationships would provide the details as to where to place these tools to achieve the desired impact.

- BIOS destruct tools pre-placed via network reconnaissance and exploitation efforts performed earlier in this two-week CNO campaign might be activated to destroy the

[66] *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Docket No. R-1128)* (Federal Reserve System, 7 April 2003): 7.
[67] Ibid.

circuit boards of key the motherboard containing the microprocessors necessary for the systems' operation.

- Chinese writings on information confrontation and network attack underscore the effectiveness of BIOS attacks as a means of destroying hardware components, such as the motherboard containing the microprocessors necessary for the systems' operation.[68]

- Tools designed to destroy the primary hard drive controller, overwrite CMOS RAM, and erase flash memory (the BIOS) would render the hardware itself completely inoperable, requiring a full replacement of motherboard components, not just an operating system reimaging, to restore the system to full functionality.

- Attacking multiple servers at a specific command, unit, or base would require the IT personnel to obtain necessary parts and physically replace the destroyed components. Performing this replacement during peacetime is a prolonged and expensive effort but during a crisis the potential delay or network outage has the potential for significant delays depending on the nature of the military unit or government agency targeted.

PLA operators do not have to achieve 100% success against all of the systems and nodes targeted. The exact minimum level of effectiveness would depend on what the desired mission outcome is; however, substantial confusion, delay, or mission degradation could possibly be achieved with a level of success far below 100 percent.

[68] Wang Zhengde , Yang shisong, Zhou Lin, p. 208.

Key Entities in Chinese Information Warfare Operations and Research

China's burgeoning information technology sector and the PLA's focus on the informationization of its force structure have led Chinese leaders to declare that the protection of the electromagnetic domain is vital to national security. Chinese leaders appreciate the growing dependence of the civilian economy on access to the international telecommunications infrastructure and military commanders understand their reliance upon advanced communications to plan and execute their missions. To ensure that critical networks are protected, the PLA has divided primary operational responsibility for network attack, defense, and exploitation between the Third and Fourth Departments of the General Staff Department for the majority of the past decade. To develop new CNO technologies and capabilities, Beijing has also turned to its maturing commercial IT sector for R&D support, sometimes using national funding vehicles to support technical research into information warfare and information security. State funding of commercial and academic research is encouraging formal R&D relationships between elite universities and industry that look similar to models used in Western defense industries to leverage the efficiencies and cost savings found in these sectors.

The PLA General Staff Department: The General Staff Deparment (GSD) is one of the PLA's four general departments directly subordinated to the Central Military Commission, the military command authority of the Communist Party's Central Committee and chaired by the Party's Secretary General. Broadly speaking, the GSD is tasked with planning, training, and organizing all aspects of the PLA's operations and shares equal stature with the General Political Department, General Armaments Department and General Logistics Department. [69] The second level of military organization in the PLA—the PLA ground forces, the PLA Navy (PLAN), PLA Air Force (PLAAF), Second Artillery (the strategic missile force), and the command of the seven geographic military regions in China—are all directly subordinate to the GSD. In addition the GSD directly oversees two important academic institutions, the Academy of Military Science and the National Defense University. The GSD is further subdivided into second tier operational departments with responsibility for specific aspects of the PLA's daily operations and planning. This study only considers those departments which open source analysis suggests have a direct role in computer network operations or the INEW mission.

Responsibility for computer network exploitation (the intelligence gathering function of CNO) and network defense appear to belong to the GSD Third Department (3PLA), China's traditional SIGINT collector. The GSD's Fourth Department (4PLA) traditionally responsible for electronic warfare, has assumed responsibility for computer network attack, most likely the result of the PLA's adoption in the past decade of INEW as its primary offensive information warfare strategy. The combination of offensive network operations with traditional

[69] David Finkelstein, "The General Staff Department of the Chinese People's Liberation Army: Organization, Roles, & Missions" in James Mulvenon and Andrew N. D. Yang, eds., *The People's Liberation Army as Organization Reference Volume v1.0* (RAND Corp., 2002): 125-133.

electronic countermeasures, itself an offensive combat function, likely made the Fourth Department the most logical bureaucratic location for these capabilities.

The June 2011 reorganization of the PLA's Communications Department into the Department of Informationization and the July 2010 establishment of the PLA's Information Assurance Base suggests that General Staff Department may now have a more formal mechanism to coordinate network operations in the PLA, even as Third and Fourth Departments retain their day-to-day operational responsibilities.

- When announcing the reorganization of the Communications Department into the Informationization Department on June 30, 2011, CMC member and Chief of the General Staff, Gen Chen Bingde stressed that the action was done to bring greater unity of effort to the process of informationization within the PLA and was not simply a name change.[70]

- An uncorroborated media report from a source with good contacts within the PLA claimed that a "cross-service Information Warfare Leadership Group" and a "Military Information Network Protection Bureau" had been established within the Communications Department as early as 2010, almost a year and a half before the PLA publicly announced the reorganization.[71]

- Small leadership groups such as this are sometimes created within the PLA and PRC civilian government to coordinate policy over a single issue crossing multiple bureaucratic boundaries. If that is the case in this situation, then it suggests the group's mandate may extend beyond purely network-electronic based activities undertaken by 3PLA and 4PLA and include other areas of IW, such as psychological warfare, public opinion warfare, and legal warfare that the PLA considers vital to achieving information superiority during a campaign.[72] Such an organizational change would be consistent with the PLA's information confrontation strategy which seeks to consolidate the command and control of the various sub-systems of information warfare under a single entity.

The Third Department of the General Staff Department (3PLA): The General Staff Department's Third Department is China's primary SIGINT collection and analysis entity,

[70] Li Yun, "*Jiefangjun Zongcanmoubu Tongxinbu Gaibian Wei Zongcanmoubu Xinxihuabu*" (PLA General Staff Department Communications Department Reorganized Into the Department of Informationization) (Xinhua, 30 June 2011).
[71] "PLA Reinforces Information and Electronic Warfare Capability" (*Kanwa Asian Defence*, February 2010).
[72] The Chinese political and military leadership conceptually considers these activities as components of information warfare, referring to them generically as "public opinion warfare" or sometimes as "The Three Warfares." PLA IW theorists advocate engaging an adversary not just on the network and electromagnetic domains but also on the cognitive domain, affecting how the adversary interprets the information they are receiving, even if the data and networks themselves are uncorrupted. The Chinese also consider that these activities that can be undertaken during peacetime to shape potential adversary perceptions such that crisis or conflict is avoided completely while still allowing Beijing to pursue its national interests. See for example: Dean Cheng, "Testimony Before the US-China Economic and Security Review Commission: China's Active Defense Strategy and Its Regional Impact." U.S.-China Economic and Security Review Commission, 27 January 2011. <http://www.uscc.gov/hearings/2011hearings/transcripts/11_01_27_trans/cheng_testimony.pdf>.

overseeing one of the largest and most sophisticated SIGINT and cyber collection infrastructures in the world and certainly the most extensive in the Asia-Pacific region. The Third Department manages at least 12 operational bureaus and three research institutes and its facilities located around China report directly to the Third Department headquarters in Beijing and are not under the administrative control of MR commanders, according to one U.S. study.[73] The Third Department is largely responsible for the PLA's computer network defense and also has a role in China's national level information security community, managing at least five information security engineering or evaluation centers.[74]

The Third Department maintains a system of several dozen ground stations capable of long range collection, specially instrumented ships, tactical mobile ground systems, and airborne platforms as well, according to analysis by other Western academic specialists and defense industry analysts.[75] Open source estimates of the Third Department's staff size vary widely, with a high end figure of 130,000 trained linguists, technicians, and researchers but the exact number remains unsubstantiated.[76] The department's technical resources, large staff of trained linguists, engineers, and analysts, and traditional absence of an offensive mission have provided it with the resources to manage the PLA's CND and CNE missions, however, little hard evidence exists in open source materials to confirm this responsibility. Activities by some units attributed to the Third Department suggest an information assurance or CND support role for the PLA and possibly a computer network exploitation or intelligence collection role.

- An uncorroborated blog posting on a military themed Chinese website noted that the Third Department maintained an Information Security Testing, Evaluation and Certification Center which certifies all PLA secrecy protection products for their security capabilities, a function that is also performed through the PRC State Secrecy Bureau. Many the Bureau's municipal and regional offices post updated lists online of the commercial firms, state-run research institutes, and academic institutions that have been awarded a certificate to manage classified computer systems and data, according to an extensive review of these sites.[77]

- This same blog posting also claimed that the Third Department previously maintained the Technical Security Research Institute of the PLA Secrecy Committee, which was formerly known as the 5th Office, 3rd Bureau of the GSD 3rd Department before the GSD's Logistics Department took over management. Interestingly the source

[73] Mark Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure" (Project 2049 Institute, November 11, 2011): 4.
[74] Ibid 5.
[75] See for example Easton 4-6; Mark Stokes, "China's Strategic Modernization: Implications for the United States" (U.S. Army Strategic Studies Institute, 1999): 32-35; and Desmond Ball, "Signals Intelligence in China," *Jane's Intelligence Review,* August 1, 1995.
[76] Easton 5.
[77] For a sampling of the content offered on many of the State Secrecy Bureau websites see the Shanghai Municipal State Secrets Bureau, www.bmj.dg.gov.cn, Guangdong State Secrets Bureau, www.bmj.gd.gov.cn, or the Liaoning State Secrecy Bureau, www.lnbm.gov.cn/.

described it is a "for-profit" organization engaging in technical secrecy research and information security equipment development.[78]

The Fourth Department of the General Staff Department (4PLA): The GSD Fourth Department, formerly the Electronic Countermeasures Department, holds an equal bureaucratic rank as the Third Department within the GSD hierarchy, but unlike the Third Department, it is charged with an offensive mission rather than a defensive electronic warfare or purely intelligence collection and analysis function. The Fourth Department was founded as an electronic warfare entity in 1990, a responsibility which includes managing a network of major research institutes involved in the R&D of new electronic countermeasure systems, the most noteworthy of which is the 54th Research Institute. The Fourth Department also maintains close relationships with China Electronic Technology Corporation (CETC) R&D organizations such as the 29th Research Institute in Chengdu, the 36th Research Institute in Jiaxing, and the 38th Research Institute in Hefei.[79] The Fourth Department also oversees the PLA Electronic Engineering Academy in Hefei which serves as the PLA's primary academic and training center for electronic warfare.

- The Fourth Department has primary responsibility for the offensive electronic-based information warfare missions in the PLA, and likely consolidated this authority in 2002 and later as INEW became the dominant strategy guiding CNA. This authority for the new mission area appears to have been hard won, occurring after a prolonged bureaucratic struggle for departmental control as reflected in a series of opposing articles in various PLA journals during this time over the future direction of information warfare and CNO strategy. The question was likely settled in favor of the Fourth Department after Major General Dai Qingmin assumed control of the organization in 2002 and was able to champion the INEW strategy he helped conceptualize.[80]

- The Fourth Department oversees ECM regiments, many of which are integrated with Group Army command structures in most military regions in China.[81] Reference in PLA media coverage to these units conducting both electronic countermeasures and CNA during large scale multi-MR and multi-group army exercises are becoming more common, likely reflecting the integration of INEW and information superiority missions with traditional firepower elements (e.g. armor, infantry, air, ballistic missiles) and a greater prominence of IW in PLA campaign plans.[82]

[78] "Highlights—PRC Military Forums in August 2011" (Open Source Center, 1 September 2011).
[79] Stokes, "China's Electronic Intelligence Satellite Developments" 18.
[80] For a more thorough analysis of this debate and the opposing positions, see James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability" in Roy Kamphausen, David Lai, Andrew Scobell, eds. *Beyond the Strait: PLA Missions Other Than Taiwan* (Strategic Studies Institute, April 2009).
[81] The PLA official press frequently refers to them as "electronic confrontation units" possibly reflecting the shift toward concepts associated with information confrontation rather than the narrower INEW precepts.
[82] Stokes, "China's Electronic Intelligence Satellite Developments" 18.

As part of the PLA's longstanding strategic focus on seizing information control of adversary C4ISR systems and command networks, the Fourth Department's primary research institutes have supported work on a variety of subjects related to countering key U.S. C4ISR systems. A survey of research published by individuals affiliated with CETC's 29th, 36th, and 38th research institutes and the Fourth Department's 54th research institute reflects work on GPS jamming, Joint Tactical Information Distribution System (JTIDS) countermeasures,[83] jamming of frequency ranges associated with communication satellites (SATCOM) commonly used by Western militaries, and synthetic aperture radar (SAR) radar jamming. Electronic warfare platforms and capabilities developed by these and similar research institutes will be coordinated with computer network attack tools against key command and control nodes and networks for comprehensive full spectrum attack.

The Ministry of Public Security (MPS): The Ministry of Public Security's active support of information security research, certification of commercial sector products for use in PRC government systems, control of commercial information security companies, and funding of academic grants for research on subjects of interest to MPS provides an important window into how the PRC state encourages and directs information security research and standards in both the Chinese commercial sector and academia. The MPS Third Institute is responsible for the creation of information security standards for all hardware and software used in the PLA and in civilian government. It also serves as the interface between MPS and various recipients of MPS sponsored grant programs and product evaluation.[84]

- The MPS 3rd Research Institute has funded specific research programs at Chongqing University on various modes of wireless security protocols, and, in cooperation with the MPS Key Laboratory of Information Network Security, provided grant funding to researchers at Fudan University that led to published research on ultra lightweight radio frequency identification (RFID) mutual authentication protocols.[85]

- The MPS 3rd Research Institute has also supported joint research projects between Zhongxing Telecommunications Corporation (ZTE), one of China's largest hardware manufacturers and Chongqing University of Posts and Telecommunications.

Technical Reconnaissance Bureaus (TRB): The PLA maintains a series of facilities known as technical reconnaissance bureaus (*jishu zhencha ju* 技术侦察局) with probable SIGINT collection missions located in the Lanzhou, Jinan, Chengdu, Guangzhou, and Beijing military regions. These facilities, likely subordinate to the Third Department, are assessed to have a tactical and strategic SIGINT collection mission each focusing on a particular geographic area of interest to Beijing. Some of these facilities may also perform aspects of the CNO missions,

[83] JTIDS is the Joint Tactical Information Distribution System (JTIDS), one of the primary datalink networks used among U.S. forces, particularly U.S. Navy and Air Force units to share targeting and threat data in real time among multiple platforms.
[84] PRC Ministry of Public Security, "Ministry of Public Security Named its First Ministerial Key Laboratories" (12 September 2008).
[85] Jin Bo, Zhang Bin, and Wang Zhihai, "Analysis and Standardization of Intranet Security Technology" (*Information Security and Communications Privacy*, July 2007).

according to an analysis of PLA media reporting, postings online by Chinese "netizens," and Western academic scholarship on the subject.[86]

A review of online resume postings and biographic information of individuals who self-identify as former TRB personnel indicates that the PLA maintains locations in the Shenyang MR, Lanzhou MR, Chengdu MR while other Western academic research has also identified additional locations in the Beijing, Guangzhou, Nanjing and Jinan MRs.[87]

- A Liaoning Province customs official working in a northern Bohai Gulf coastal city notes in his online professional biography that he worked as a Russian translator at the Shenyang MR technical reconnaissance bureau after completing Russian language studies at the PLA Foreign Languages Institute, the Third Department's training center. This language background suggests both the regional collection focus and a likely COMINT mission at the Shenyang facility.[88]

- A former PLA software developer assigned to the Shenyang TRB indicated in his profile on a job search website that he completed graduate computer science training at the PLA's Information Engineering University, one of the leading PLA academic institutions for computer science and a center of advanced research on information warfare. He also worked with an information security research center at the university prior to taking his assignment.[89]

- A municipal website for Qilihe City in Gansu Province highlighted a 2009 visit by the political commissar from the Lanzhou MR Technical Reconnaissance Bureau to the city's officials, including the mayor and his staff. [90]

- A blog posting of a PLA document noting personnel assignments and promotions for May 2009 identified Chengdu as the location of the 1st Technical Reconnaissance Bureau for an individual assigned to the unit as its political commissar.[91]

- In September 2008, personnel from a Technical Reconnaissance Bureau in the Chengdu MR received multiple awards for "S&T progress" and achievement in

[86] Dennis Blasko, "PLA Ground Force Modernization and Mission Diversification: Underway in all Military Regions." in Roy Kamphausen, Andrew Scobell, eds. *Right Sizing the People's Liberation Army: Exploring the Contours of China's Military* (Strategic Studies Institute, September 2007): 366-372.
[87] Author conversations with Mr. Ellis Melvin; see Ellis Melvin, "A Study of the Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureaus," June 19, 2005; Dennis Blasko, "PLA Ground Force Modernization and Mission Diversification: Underway in all Military Regions." in Roy Kamphausen, Andrew Scobell, eds. *Right Sizing the People's Liberation Army: Exploring the Contours of China's Military* (Strategic Studies Institute, September 2007): 366-372; Stokes, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure" 11.
[88] See Profile posting at http://yk.lnciq.gov.cn/ldxx/hhb; "*Chongqing Shi Wanzhou Qu Di San Jie Ren Da Daibiao—Jiang Jian*" (Third People's Congress Chongqing Wanzhou District Representative—Jiang Jian) (Baidu, viewed November 2011).
[89] In his online resumé, this individual identifies himself only by his surname Yang. See Job592.com, "Yang" <http//www.job592.com/cv/081004/person60007.html>.
[90] "Lanzhou MR 1st Technical Reconnaissance Bureau Visits Qilihe" (Qilihe People's Government Affairs, 20 January 2009).
[91] "*Budui 5 Yue Renshi Biandong Huizong*" (Summary of Personnel Changes May 2009) (14 June 2009).

connection with a "computer workstation security protection system," according to official Party media affiliated with the Chengdu MR.[92] The awards suggest that the unit is staffed by personnel with sophisticated technical skills able to conduct original research in areas of information security.[93]

Military Region	Unit Designator	Location	Military Unit Cover Designator
Beijing MR HQS	Beijing Military Region Technical Reconnaissance Bureau	Beijing	66407 Unit
Chengdu MR HQS	1st Technical Reconnaissance Bureau	Chengdu, Sichuan Province	78006 Unit
	2nd Technical Reconnaissance Bureau	Kunming, Yunnan Province	78020 Unit
Guangzhou MR HQS	Technical Reconnaissance Bureau	Guangzhou, Guangdong Province	75770 Unit
Jinan MR HQS	Technical Reconnaissance Bureau	Jinan City, Shandong Province	72959 Unit
Lanzhou MR HQS	1st Technical Reconnaissance Bureau	Qilihe District, Gansu Province	68002 Unit
	2nd Technical Reconnaissance Bureau	Urumqi, Xinjiang Uighur Autonomous Region	69010 Unit
Nanjing MR HQS	1st Technical Reconnaissance Bureau	Nanjing, Jiangsu Province	73610 Unit
	2nd Technical Reconnaissance Bureau	Fuzhou, Fujian Province	73630 Unit
Shenyang MR HQS	Technical Reconnaissance Bureau	Shenyang City, Liaoning	65016 Unit

Figure 1: PLA Military Region Headquarters Technical Reconnaissance Bureaus[94]

[92] "Chengdu Military Region (MR) 78006 Unit Excels In Informatization Building" (*Chengdu Zhanqi Bao*, 24 September 2008).
[93] See Ellis Melvin "A Study of the Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureaus."
[94] The authors wish to express their appreciation to Mr. Ellis Melvin for his assistance with the information on China's Technical Reconnaissance Bureaus. This table was assembled in part from information developed by Mr. Melvin, whose open source research on PLA unit histories and activities and careful databasing of information culled from the unclassified record has been of invaluable assistance in this study. See Ellis Melvin "A Study of the Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureaus." See also Stokes, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure."

- Guangzhou MR Technical Reconnaissance Bureau held training for new unit members on a variety of technical subjects designed "to enhance information offense and defense," according to official party affiliated media.[95]

Technical research by individuals who indicate affiliation with a TRB and official PRC media reporting on the activities of these units suggests active research interests in computer network defense and a role in information security for other PLA units.

- A researcher who published work on an improved multi-pattern matching algorithm for precise pattern matching strings in intrusion detection systems identified himself as an assistant engineer with the 72959 Unit (Jinan MR Headquarters TRB); the paper's co-authors are identified as faculty members at the PLA Information Engineering University.[96]

- Guangzhou MR Technical Reconnaissance Bureau personnel based at a Hainan Island have been noted in media sources receiving awards for network related research including internet viruses and voice over internet protocol (VOIP) research.[97]

- A November 2009 photo essay in Zhanqi Bao, a newspaper published by the General Political Department in the Chengdu MR shows members from the 78006 Unit (Chengdu 1st TRB) conducting what is claimed to be an information security check at an unnamed PLA facility.[98]

Information Warfare Militia: The PLA leadership guidance on informationization encompasses more than just operational active duty units. Informationization is also transforming the PLA's traditional forms of mobilization and civil-military integration, under a rubric sometimes referred to within the PLA as "people's war in a new era." Consequently, the modernization of the militia and reserve forces is largely focused on recruiting new members with skills in essential high technology areas, in part to form new units but also to help transform existing militia or reserve units by incorporating recruits with advanced education and technical skills in mission critical areas.

- The 2006 National Defense White Paper first noted that the priority for militia force building would be to increase the recruitment numbers of reservists and militia members with high-tech backgrounds in all service arms.[99]

[95] "75770 Unit Holds Training Assemblies On New Training Program" (*Zhanshi Bao*, 11 December 2008).
[96] Sun Xiaoyan, Wu Dongying, Zhu Yuefei, and Guo Ning, "Research and Improvement of Wu-Manber Multi-pattern Matching Algorithm" *Jisuanji Gongcheng* (Computer Engineering) (1 April 2008): 85-86,89.
[97] Stokes, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure" 12
[98] "78006 Unit Conducts Information Security Check in Office Facilities" (*Zhanqi Bao*, 13 November 2009): 1.
[99] Information Office of the State Council of the People's Republic of China, "China's National Defense in 2006" (29 December 2006).

- The militia is administered at four levels within the PLA to provide the means of mobilizing support and integrating militia members into provincial military commands, prefectural military commands, people's armed forces departments of counties (county-level cities or municipal districts) and basic-level people's armed forces departments.

The 2006 Defense White Paper identified an explicit change in militia building strategy to shift recruiting and training from rural areas, where it has traditionally been, to urban areas for the express purpose of taking advantage of the large pools of talent in the commercial high tech sectors.

- Militia building since 2006 has begun to focus on creating specialized units over less-skilled infantry units and is expanding away from the reliance on employees from state-owned enterprises to private sector high tech industries to meet the need for personnel in units such as communications, reconnaissance, and information technology.[100]

To meet these recruiting requirements, the PLA has turned to its growing pool of tech-savvy civilian talent for recruitment into its militia forces. While 2006 was the first formal declaration of this new militia building strategy, the practice of seeking recruits from high-tech industries, particularly information sciences, has been underway at the local level since at least 2002, and has been meeting with apparent success according to a review of PLA reporting on militia building.[101]

- As early as 2005, Guangzhou MR People's Armed Forces Departments, the local level coordinating and administrative body for militia units began surveying and registering technical personnel in their respective areas to understand the resources available to them and to encourage greater participation in militia units or civilian mobilization exercises, according to 2006 article in a Guangzhou provincial party newspaper.[102]

- Nanjing MR official media as early as 2005, reported on efforts to recruit individuals with advanced graduate degrees in computer science to establish more information warfare militia units, suggesting that the PLA is assigning these units tasks which are far more sophisticated than simple monitoring of network defense sensors or maintenance of communications systems as part of occasional training.[103]

[100] Ibid.
[101] Ye Youcai and Zhou Wenrui, "Building a High-quality Militia Information Technology Element" *Guofang* (National Defense, 15 September 2003).
[102] "Manpower Mobilization Capability Should Be Improved by Strengthening Three Areas" (*Guangzhou Zhanshi Bao*, 7 December 2005).
[103] Xu Changdu and Zhang Zhidong, "High-Tech Militia Detachments Cannot Become 'Militia Detachments on Display'" (*Renmin Qianxian,* 25 March 2005).

Details of IW militia exercise activities, though rarely noted explicitly in PRC media, provide some indication that the PLA intends to integrate these units into broader campaign plans and is working to integrate militia units with active duty units in some cases, consistent with information confrontation principles that the PLA is moving toward adopting.

- One report in an official Communist Party newspaper in Nanjing noted the presence of a 50 person IW militia unit based in Shanghai comprised of IT professionals drawn from local Shanghai companies that participated in a 2009 online training simulation. Militia members were integrated into a "Red Force" unit and provided both CNA and CND support against a Blue Force unit's command and control infrastructure, reflecting the potential mission and targeting focus of these groups.[104]

The ability to pull from the ranks of China's burgeoning and increasingly sophisticated IT industry in major urban areas will allow the PLA to augment the capabilities of active duty information warfare troops or expand the numbers of targets that can be managed, especially if militia units participate in peacetime network exploitation activities as a component of their regular duties. Regardless of their specific missions, the change of mobilization and recruitment strategy by the PLA has resulted in an expansion of militia units involved in all aspects of computer network operations.

- By late 2005, the Chengdu MR had created over 290 separate electronic warfare, network warfare, and psychological warfare units as the result of integrating staff from local information technology companies, according to an official PLA media source published by the General Political Department,[105] a trend that if copied in areas with significant urban populations or with strong IT industrial bases could represent a dramatic expansion in the numbers of available teams that the PLA can potentially draw on as mission requirements dictate.

Consistent reporting over almost eight years on the establishment of civilian-staffed information warfare militia units leaves little doubt that these units are a permanent addition to the PLA's information warfare force structure. The use of commercial industry as a source of personnel is likely allowing the PLA to form relationships at the local level with key high-tech commercial companies while simultaneously gaining access to to personnel with essential technical skills.

What remains unclear from the open source record is the PLA's command and control structure for IW militias. The scope of the recruitment and modernization efforts underway suggests that the PLA is also likely working to develop an employment strategy for these units

[104] Li Li and Liu Zongfeng, "New-Type Militia Detachments 'Draw Swords' on Ground, at Sea, in Air and in Space" (*Nanjing Renmin Qianxian* (Nanjing People's Frontline), 28 September 2009): 4.
[105] Jiang Xueyou, "Enhancing Functional Awareness, Strengthening Direction of Work - Mobilization Department Director of Military Region Headquarters Department Ling Feng Talks About National Reserve Forces Building" (*Chengdu Zhanqi Bao*, 29 December 2005): 1.

during wartime. One of the PLA's key tactical considerations is mission assignment and deconfliction with other CNO teams. Without some formal means of coordinating network operations activities among active duty and militia CNO teams, the PLA increases the risk of "electronic fratricide" if these groups inadvertently expose or corrupt each other's sensitive operations during a campaign.

Finally, the open source record in both the PRC media and PLA writings is unclear whether PLA leaders consider a highly trained IW militia unit with the capability for sophisticated operations as a strategic asset directly subordinate to the military region command (or higher, as some ECM regiments appear to be), or whether IW militia units will be subordinate to lower echelons of command. The question is more than an arcane academic debate among China military specialists; it may have implications for the types of CNA and CNE missions that these teams are assigned, what they target, and how deeply the potential expertise on these teams will be mined by military commanders.

State-Sponsored Computer Network Operations Research in Chinese Academia

China's strategy to enhance its IW technical and operational foundation and for broader advancements in informationization within the military has focused on blending the resources of state, civil, and military sectors to achieve growth in areas identified as critical strategic capabilities. The nexus of the government political ministries with civilian universities represents one element of this strategy. University support to IW related research for the PLA or other areas of the PRC government is extensive and covers a range of information security and information warfare topics.

The PLA's use of the expertise resident within its academic community has allowed it to acquire cutting edge capabilities such as the world's faster supercomputer, consistent technical standards for the evaluation of information security products used in government, and has created a conduit for highly trained talent to join the ranks of government research institutes, private industry, and the military including IW militia units. This strategy to leverage all aspects of IT expertise and funding sources is paying dividends now as more universities take on IW research projects via state grants and commercial IT companies see the benefits of greater R&D collaboration with state and academic entities.

Military University IW Research and Development

Much has been written about PLA professional universities and academies, their curricula, faculty, and research initiatives with regard to computer network operations. This section will briefly review the scope and approach of key organizations relevant to computer network operations.

Academy of Military Sciences: The Academy of Military Sciences, located in Beijing and answering directly to the Central Military Commission, is the PRC military's main body for military science research and strategy and doctrine development. AMS carried out some of the earliest studies of computer network operations but maintains a more academic rather than tactical or operational training role.[106] Recent AMS research studies relevant to information warfare focus on the operational use of computer network exploitation, U.S. network-centric warfare models, and foreign military information management structures.[107]

National Defense University: The National Defense University (NDU), located in Beijing, trains the nation's military command leaders and conducts research on the application and training

[106] James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability" 275-276.

[107] LTC Liu Zhongbao, "Data Mining: An Important Technique for Seizing Information Superiority"; Meng Fanjun, "Network-centric warfare: the American way of war in the information age"; and Wang Baocun, "An Exploratory Analysis of Chief Information Officer Systems In Foreign Militaries," in *National Defense and Armed Forces Building in the New and Century New Age* (Military Yiwen Press, 2008).

of new concepts in military science to the current military force. It serves a more command than academic role, but NDU researchers collaborate with scholars from numerous other organizations including AMS and Technical Reconnaissance Bureau personnel.[108] Recent NDU research studies relevant to information warfare focus on foreign military informatization and information warfare approaches.[109]

Wuhan Communications Command Academy: The Wuhan Communications Command Academy, (CCA) located in Wuhan, Hubei Province, is the PLA's only mid-level communications command institution. CCA trains Third Department mid-level communications command and automated management personnel in information warfare and military communications systems and develops operational doctrine for information operations.[110] Recent scholarship at CCA relevant to information warfare includes studies of Internet routing scalability, wireless Internet use in military environments, data mining techniques, distributed denial of service attacks, and U.S. network-centric warfare planning. CCA researchers' recent collaborations on information operations related topics include those with scholars from Tsinghua University, the PLA Information Engineering University, PLA Unit 61081, Huazhong University of Science and Technology, Wuhan University of Technology, and the PLA University of Science, Xi'an Communications Academy, the China Institute of Electronic System Engineering, and the PLA Air Force Dalian Communication Officer School.[111]

National University of Defense Technology: The National University of Defense Technology (NUDT), located in Changsha, Hunan Province, is a technology-oriented university heavily involved in military research and development, jointly administered by the Ministry of National Defense and the Ministry of Education. NUDT, the development center for China's Tianhe-IA supercomputer, lists among its key research areas electronic and information warfare target recognition in addition to biometrics, nanotechnology, quantum computing, and non-linear mathematics.[112] NUDT faculty include professor Fang Binxing (方滨兴), often called the "Father of the Great Firewall,"[113] who also holds a professorship at Harbin Institute of Technology, numerous directorships, and is a board member of various national computer network engineering and security-related government advisory committees including the Informationization Advisory Committee of the PLA General Logistics Department.[114] NUDT researchers' recent collaborations on information operations related topics include those

---

[108] Ibid; NDU researcher Guo Qingbao (郭庆宝), for instance, co-authored a 2008 study on informationization with Zhuang Juanjuan (庄娟娟) of Jinan MR unit 72959 (3rd Technical Reconnaissance Bureau). See Guo Qingbao and Zhuang Juanjuan, "Major steps in accelerating informationization in the South Korean military," *National Defense and Armed Forces Building in the New Century and New Age* (Military Yiwen Press, 2008).

[109] Li Li, "A preliminary exploration of models and patterns for informationization in foreign militaries," *National Defense and Armed Forces Building in the New Century and New Age* (Military Yiwen Press, 2008); Guo Qingbao and Zhuang Juanjuan, "Major steps in accelerating informationization in the South Korean military."

[110] Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability" 276.

[111] CNKI, <www.cnki.net>.

[112] PRC National University of Defense Technology, "*Jichu Yanjiu Zhongdian Yanjiu Lingyu He Fangxiang*" (Areas and Directions of Basic and Key Research) and "*Zhuyao Yanjiu Fangxiang*" (Main Research Directions).

[113] Fan Yunyu, "Great Firewall Father Speaks Out" (*Global Times Online*, 18 February 2011).

[114] Harbin Institute of Technology, "Full List of Professors"; "*Beijing Youdian Daxue Xiaochang Fang Binxing Jianjie*" (Profile of Beijing University of Posts and Telecommunications Professor Fang Binxing) (Renmin Wang, viewed November 2011).

with scholars from Beijing University of Technology, Wuhan University, Shanghai Jiao Tong University, PLA Information Engineering University, and the PLA's 63880 Unit.[115]

- The PLA 63880 Unit, a Luoyang electronic countermeasures training and development unit subordinate to the General Armaments Department (GAD), has served as an ECM blue force for other PLA units training at this base and developed new unspecified ECM equipment in collaboration with "specialized technical forces of S&T research institutes in China," possibly a reference to NUDT personnel.[116]

- NUDT faculty have regularly collaborated with 63880 Unit personnel on a variety of advanced R&D topics related to radar and electronic countermeasures, including work on phased array radars, data fusion algorithms, SAR radar detection of ballistic targets, and jamming techniques.[117]

- Perhaps NUDT's most successful partnership has been with Longson Technology Co. (龙芯), designer of the fully domestic Longson chip, also known as the Godson chip, incorporated into the Tianhe-1A, judged in late 2010 as the world's fastest supercomputer.[118] The development of this system within China's military R&D community is a strong indication of its intended dual use applications.

Information Engineering University: The PLA Information Engineering University (PLAIEU), located in Zhengzhou, Henan Province, is perhaps the military university with the most comprehensive involvement in information warfare and computer network operations training, planning, and possibly also execution. According to a 2008 *PLA Daily* description, the school employs 800 professors and senior engineers and 100 part-time professors, serving 55 graduate degree programs.[119] Published PLAIEU-sponsored research includes studies on worm propagation, network attack evaluation, kernel-mode rootkits, data hiding, malware behavior detection, and "emergency public opinion control."[120]

PLAIEU achieved worldwide notoriety in August, 2011 when the user 'chinesecivilization2' posted to YouTube a segment of the military-themed television documentary, "The Network

[115] CNKI, <www.cnki.net>, Chen Feng et al, "Two Formal Analyses of Attack Graphs," *Journal of Software*, 1 April 2010, p.838.
[116] Han Xinwen, Gao Junguang, and Yang Baoqing. "Application Study of Information Countermeasures 'Blue Force' in Base Training." *Junshi Yunchou Yu Xitong Gongcheng* (Military Operations Research and Systems Engineering) 24 2 (June 2010): 75-78.
[117] See for example: Jin Guanghu, Gao Xunzhang, Li Xiang, and Chen Yongguang, "ISAR Image Cross Scaling Method for Ballistic Targets Based on Image Registration" *Xitong Gongcheng Yu Dianzi Jishu* (Journal of Systems Engineering and Electronics) (1 December 2010): 2565-2569; Wang Jixiang, Liu Guizhong, and Feng Ying, "Evaluation of Jamming Effect of AM Communications Based on Modulation and Recognition Features" (*Junshi Yunchou Yu Xitong Gongcheng* (Military Operations Research and Systems Engineering)): 75-78; and Han Xinwen, 75-78.
[118] "Made in China processors power world's fastest supercomputer" (*Want China Times*, 25 March 2011).
[119] "Information Engineering University" (China Military Online, March 2008).
[120] Tang Jun et al., "Simulation Study on Worm Propagation Characteristics" (*Xitong Fangzhen Xuebao,* 9 December 2010); Cao Yan et al., "Fuzzy Evaluation Model for Effectiveness of Network Attack Based on Generalized Operators" *Jisuanji Yingyong Yanjiu*, 1 August 2009); Ding Liang et al., "Research on Covert Techniques of Kernel-Mode Rootkits Under Windows" (*Jisuanji Gongcheng Yu Sheji* (Computer Engineering and Design), October 2006).

Storm is Coming," broadcast by CCTV-7 on July 16, 2011. The segment showed the live use of an apparent denial of service tool, bearing the title "PLA Information Engineering University" in Chinese, and offering the user a list of "attack destinations" including a Falun Gong website hosted at the University of Alabama in Birmingham (UAB). The broad exposure gained by the video's YouTube distribution brought considerable attention to the PLAIEU, convincing many that the school sponsored hacking activity outright. However, staff at UAB later commented that the computer identified in the video had not been compromised, suggesting that the video only showed a simulation. Nevertheless, the video strongly suggests that the PLAIEU is involved in developing software to assist network attack operations. The specificity of the example (a Falung Gong website at an Alabama university) reflects the detailed, real world network reconnaissance that Chinese network security researchers in both academia and government are conducting to further PRC security interests.[121]

PLAIEU researchers are prolific publishers of information security-related material, having issued more than 300 articles in the past two years. Their recent collaborations include those with scholars at Zhengzhou University of Light Industry, PLA Unit 61365, Luohe Medical College, Public Security Marine Police Academy, Xi'an University of Electronic Science and Technology, Hebei University of Science and Technology, Sichuan University, the National Digital Switching Engineering Center, Nanyang Normal College, and many others. The number and diversity of collaboration partners enjoyed by PLAIEU researchers suggests both aggressive partnership-building on the school's part and a broad-based reputation for technical expertise.[122]

Although the above key military institutions play important roles in the development of China's information warfare capabilities, the PLA's development of new CNO and EW capabilities depends to a substantial degree on collaboration with civilian academic institutions for the modernization of military command and technical talent.[123]

Civilian Universities

A review of PRC university technical programs, curricula, research foci, and funding for research and development in areas contributing to information warfare capabilities illustrates the breadth and complexity of the relationships between the universities, government and military organizations, and commercial high-tech industries countrywide. The network of institutions and scholars funded to conduct research into information warfare techniques and technologies extends beyond the most elite schools (although those are at the core) to

[121] For a skeptical account of the incident, see Joel Herrick, "CCTV documentary reveals hacking tool, links Chinese government to cyber attacks" (Shanghaiist, 24 August 2011). The original YouTube video can be found at <http://www.youtube.com/watch?v=L_Wu1HIZbBk>. For the University of Alabama response, see "Slip-Up in Chinese Military TV Show Reveals More Than Intended" (*The Epoch Times*, 21 August 2011).

[122] CNKI, <www.cnki.net>.

[123] One example is a 2009 Guangzhou MR study that cross-pollinated military personnel into civilian technical and broader academic training, including "information network" training, to develop professional talent and thereby ease military transformation. See Zhang Yang, "Opening Up Rich Soil at the Front Lines to Nurture Talent" (*PLA Daily*, 1 February 2009).

smaller, specialized schools, suggesting a continuing expansion of high-tech skill communities into niche areas of the national economy, such as finance, education, and law.

Government funding of university R&D in areas related to computer network operations is part of a broader national strategy to combine elements of state, military, and civil society to modernize China's information systems infrastructure and information warfare capabilities. The national leadership is leveraging science and technology (S&T) resources from the civilian IT sector, military universities, military research and development institutes, civilian academia, and active duty PLA units to support a variety of research initiatives related to IW.

In the civilian academic environment, the PRC government—in concert with the PLA in some cases—uses at least five established national grant programs to fund research related to information warfare and to the PLA's informationization programs. Whereas funding from some of these programs is disbursed to researchers at a broad collection of academic institutions, certain grant programs appear to be concentrated among a select group of universities and research centers. ***We assess that national information security grants are frequently awarded to these universities partly due to possible patronage relationships between the sponsoring government ministries and key faculty within university research centers, and because of their ability to apply the research to multiple programs aligned with national high-technology priorities, including the modernization of state secrecy, the technical professionalization of the PLA, and the continuing development of information conflict capabilities.***

- The establishment of State Secrecy Academies at Nanjing University, Harbin Institute of Technology, Sun Yat-Sen University, and Northwest Polytechnic Institute is based on the ability of the State Secrecy Bureau/MIIT sponsored academies to draw from those universities' "resources in information technology, information engineering, and network security to support national information security efforts, and to groom reliable talents in that field."[124]

- Harbin Institute of Technology, benefiting from the widest array of national information security grant vehicles (a total of five) in addition to hosting a State Secrecy Academy, also sponsors one of only a few Information Conflict Laboratories found nationwide, with strengths in steganography and information processing technology.[125]

- Southeast University, in Nanjing, Jiangsu Province, another school supporting information security research with a broad array of national-level information security grants, cites as the main purpose of its national-level grant funding to develop high-tech talent for "government-funded schools, state-owned scientific

[124] Wang Fanhua, "The First State Secrecy Academy in Western China Established at Northwestern Polytechnical University" (Northwest Polytechnical University, 12 January 2011). The MIIT, or Ministry of Industry and Information Technology, was founded in 2008 to consolidate the oversight of the national defense and information technology industries.
[125] Harbin Institute of Technology. "*Xinxi Duikang Jishu Yanjiu Shi*" (Information Conflict Technology Laboratory).

research institutions, state key enterprises, government agencies, government-funded public institutions, and PLA units."[126]

At least 46 civilian universities found to conduct information security research nationwide benefit from one or more of roughly five main national-level high technology grant programs, reflecting what appears to be a broad-based technology development direction consistent with published national planning priorities. Of these, approximately ten schools receive funding from three or more programs, and three schools – Southeast University, Harbin Institute of Technology, and Zhejiang University – receive funding from all five of the programs reviewed. The concentration of information security funding in a handful of schools suggests that grant-giving institutions such as the National Natural Science Foundation, the Ministry of Education, the Ministry of Industry and Information Technology, and the Ministry of State Security have selected key faculty and research centers through which to sponsor sensitive research and development with information security and information warfare applications (see Appendix A for a list of universities using national grant programs to support research with IW applications; and their associated grant programs).

- The 863 National High Technology Research and Development Program (*guojia gaojishu yanjiu fazhan jihua;* 国家高技术研究发展计划) was established in March, 1986 to promote national technological independence through the advancement of advanced science and technology research in areas including information technology and telecommunications and many defense related and dual use projects. 863 Program funding, the most popular and widespread among the key programs supporting information security research, sustains both civilian and military-oriented research and development conducted at civilian universities.[127]

- The 973 National Key Basic Research Program, or "973 Program" (*guojia zhongdian jichu yanjiu fazhan jihua;* 国家高技术研究发展计划), is a national-level grant program managed by the PRC Ministry of Science and Technology (MOST), established in 1997 "to organize and implement basic research to meet the nation's major strategic needs" in various areas of scientific application including information science. 973 projects include research across scientific domains overseen by designated government ministries, often the Ministry of Education or one of its provincial branches, with research teams often spread across numerous universities.

[126] Southeast University, "*Guanyu Yinfa 'Dongnan Daxue 2010 Nian Biye Yanjiusheng Jiuye Banfa' He 'Dongnan Daxue 2010 Jie Benke Biye Sheng Jiuye Banfa' De Tongzhi*" (Notice Concerning "Job Placement for Southeast University's 2010 Graduate Students" and "Job Placement for Southeast University's 2010 Undergraduate Students") (2009).
[127] PRC Ministry of Science and Technology, "*Guojia Gao Jishu Yanjiu Fazhan Jihua (863 Jihua)*" (The National High-Tech Research and Development Program). See for example funded research projects conducted at the Computer Network and Information Security Technical Research Center at Harbin Institute of Technology, supported by "863 (military and civilian)."

- Current 973 project areas include broadband wireless communication, trusted cloud computing, the Internet of Things, integrated networks, and network virtualization. They are led by scholars from the PLA Information Engineering University, Tsinghua University, Harbin Institute of Technology, Shanghai Jiao Tong University, and other civilian universities attracting the majority of focused national-level information security research funding.[128]

- The National 242 Information Security Program (*guojia 242 xinxi anquan jihua xiangmu;* 国家242信息安全计划项目), administered by the Ministry of Industry and Information Technology, appears to be focused on government-sensitive information security projects. Information about this program can only be gleaned from faculty biographies and resumés posted online, and the titles and descriptions of many of the projects funded by this grant program are redacted.[129] At some universities surveyed for this study, 242 Program applications and information were provided to students through university military offices, suggesting localized military supervision of 242 Program applicants and projects.[130]

- Information on the Ministry of State Security 115 Program (国家安全部115), also known as the National Ministry of State Security 115 Program, like the 242 Program, can only be learned by surveying resumés, program and faculty profiles, and research center award applications to the PRC Ministry of Education. This program appears to be focused on highly sensitive information security research, as evinced by the frequent redaction not only of project titles, but also of project grant numbers themselves.[131] Resumes sometimes note simply that the individual worked on a 115 State Security Program project followed with the topic listed as "confidential," or "secret," (*baomi* 保密 *or mimi* 秘密).

- Sponsorship and administration of the National s219 Information Security Application Demonstration Project (*guojia s219 xinxi anquan yingyong shifan gongcheng* 国家s219信息安全应用示范工程) is also difficult to ascertain, although information security researchers at no fewer than ten of 46 identified Chinese universities conducting information security research have been funded by this program. s219-funded projects include research on intrusion detection technology conducted at Beijing University; research on "e-Security Platforms"

[128] PRC Ministry of Science and Technology, "*Guojia Zhongdian Jichu Yanjiu Fazhan Jihua*" (The National Key Basic Research Program).
[129] See for example an entry in the resumé of one Chinese Academy of Sciences researcher: Ding Guodong, "*Mianxiang Luntan He Xinwen De (redacted) Jiance*" ((redacted) Monitoring of Forums and News) (Chinese Academy of Sciences).
[130] Xi'an Jiao Tong University, "*Guanyu Shenbao Guojia 242 Xinxi Anquan Jihua Xiangmu De Tongzhi*" (Notice Concerning Reports of the National 242 Information Security Program) (June 2006).
[131] See for example "*2009 Niandu Shuangyu Jiaoxue Shefan Kecheng jianshe Xiangmu Shenbao Biao—Shujuku Xitong Ruanjian Gongcheng*" (2009 Bilingual Education Demonstration Course Development Project Report—Database System Software Project) (Beijing Jiaotong University, 26 May 2009); Jiang Rui and Song Yubo, "Dongnan Daxue Kewai Yanxue Jiangzuo" (Southeast University Extracurricular Research Lecture Series).

conducted at Shanghai Jiao Tong University; and research on virtual private networks (VPNs) conducted at Southeast University.[132]

- In addition to the above national-level grant programs, many scholars support their information security research with provincial, local, and private grants. These are exemplified by programs such as the Jiangsu Province Administration Program for the Protection of State Secrets, the Shanghai City Scientific and Technological Program, and the Huawei Foundation Program (see Appendix B for an extensive list of grant programs found to support information security research with information warfare applications).

[132] Shanghai Jiao Tong University, "Zheng Dong."

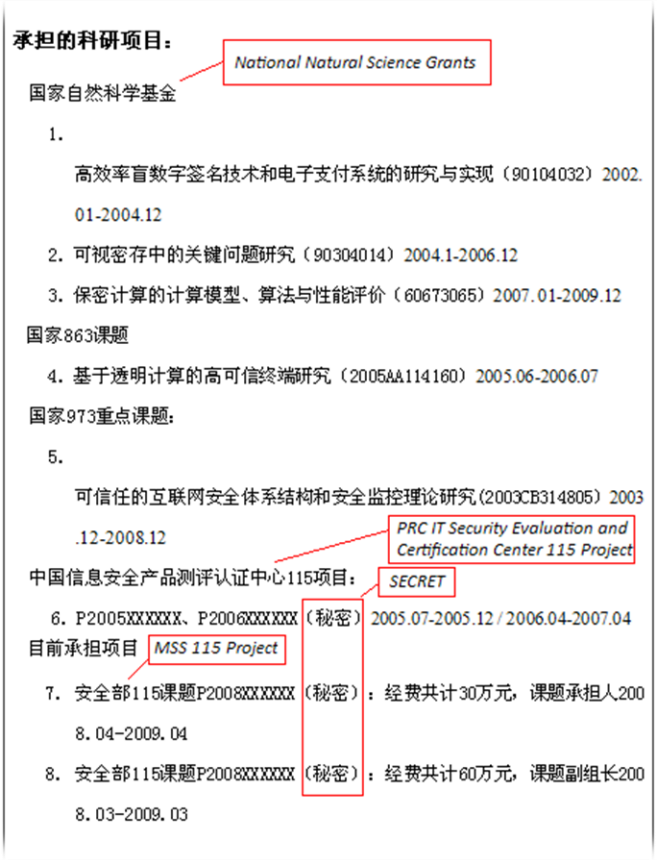

Figure 2: Descriptions and obfuscation of 115 Project grants awarded to Liu Duo, Lecturer at Beijing Jiao Tong University. Source: Wang Fangshi, "2009 Bilingual Education Model Curriculum Project Report," 26 May 2009.[133]

The grant program goals generally align to the strategic priorities of the 11th and 12th Five Year Plans (2007–2010 and 2011–2016 respectively), reflecting the importance that the PRC political leadership has placed on enhancing high technology capabilities, including informationization within the PLA, and particularly on improving national technical information warfare capabilities.

- 973 Program priorities addressing information security are aligned with the five-year national plans in broad terms of national security requirements and domestic technological innovation, including next-generation Internet technologies. This is reflected in the program's currently announced research areas, which include "system

[133] <sy.zlgc.org/upload/20090531170518828.doc>.

of systems" integration and new network technologies employing universal standards.[134]

- According to some interpretations of the current national plan, 863 Program support for research into high performance computing reflects the implementation of the "Long-term Scientific and Technological Development Plan," some key tasks of which are expressed in areas of the 12th Five Year Plan. [135]

Most universities conducting research applicable to advancing IW capabilities are receiving funding from only one or two grant vehicles. However, at least ten institutions are receiving funds from three or more national level grants for IW themed research, suggesting that these institutions are primary centers of not only research and development for CNO capabilities, but also are likely grooming the country's next generation of top tier talent in these fields.

- **The Harbin Institute of Technology or HIT** (*haerbin gongye daxue;* 哈尔滨工业大学), founded in 1920, enjoys favorable treatment from the central government. The university operates at least nine research centers focused on technical areas related to information warfare capability development, including the Center for Information Retrieval, Network and Information Center, School of Software, and the Network and Information Center. HIT hosts one of only four national State Secrecy Academies, and appears to be well-connected to government military and security communities, including the PLA. It advertises close relationships with alumni General Huang Yongqin (黄永勤), Director of the GSD Third Department's 56th Research Institute, Luo Wei (罗为), Director of the PLA GSD Technology Department, and with Ding Mingfeng (丁明峰), General Manager of ZTE.[136] Harbin Institute of Technology is a regular recipient of national grants supporting research on "major national security projects," underscoring the importance of this institution to the PLA's continued modernization of its CNO tools and practices and suggesting that the research being done here merits careful attention by those following Chinese developments in this field.

- **Southeast University or SEU** (*dongnan daxue;* 东南大学), located in Nanjing, Jiangsu Province, is a National Key University administered directly by the Ministry of Education. Southeast University operates a Department of Computer Science and Engineering with a teaching staff of 18 graduate assistants, 24 full professors, and 35 associate professors; a School of Information Science and Engineering with a teaching staff of 23 graduate assistants, 41 professors, 36 associate professors; and a College of

[134] Ming Yi Business Consulting (Beijing). "*973 Jihua Zai Shiyi Wu Qijian De Zhidao Fangzhen*" (Program Guidelines in the Eleventh Five-Year Plan); PRC Ministry of Science and Technology, "*Yiti Hua Kexin Wangluo Yu Pushi Fuwu Tixi Jichu Yanjiu*" (Basic Research in Integrated Trusted Networks and Universal Service Systems).
[135] PRC Ministry of Science and Technology, "*Guanyu Zhengji Shi'er Wu 863 Jihua Gaoxiao Neng Jisuanji Ji Yingyong Fuwu Huanjing Zhongda Xiangmu Keti Jianyi De Tongzhi*" (Notice Concerning a Call for 12th Five-Year Program 863 Program Major Projects on High-Performance Computing and Application Server Environments).
[136] Harbin Institute of Technology. "*Benke Sheng Zhaosheng*" (Undergraduate Admissions).

Software Engineering with a teaching staff of 18 graduate assistants, 27 professors, 37 associate professors, and 28 lecturers, quite a large allocation of resources focusing specifically on areas supporting the continuing development of IW capabilities. Southeast University cites as the main purpose of its national-level grant funding to develop high-tech talent for "government-funded schools, state-owned scientific research institutions, state key enterprises, government agencies, government-funded public institutions, and PLA units."[137]

- **Beijing University of Posts and Telecommunications or BUPT** (*beijing youdian daxue;* 北京邮电大学) was founded in 1955 as a key telecommunications research center affiliated with the PLA General Staff Department. Now independent, the school continues to specialize in telecommunications and has branched out into computer science and information security. BUPT enjoys strong government ties, thanks in part to the position and reputation of its university president, Fang Binxing (方滨兴), a renowned information security expert who conceived and developed China's "Great Firewall" national Internet monitoring system. BUPT operates a School of Information and Communication Engineering, a School of Computer Science, a School of Software Engineering, and a School of Automation, all engaged in research and development contributing to the development of China's information warfare capabilities.[138]

- **Shanghai Jiao Tong University or SJTU** (上海交通大学), founded in 1896, concentrates significant talent in its Computer Science and Engineering Department's "Crypto Group," which conducts advanced research into cryptography and information security. This group maintains a Cryptography and Information Security Lab, headed by Chen Kefei (陈克非), which lists a portfolio including research into authentication protocols and sensor network security. It also runs a Cryptography and Computer Security Lab, headed by Gu Dawu (谷大武), which sponsors research into technical areas including side channel attack implementation, reverse engineering, cryptography analysis and design fundamentals. In addition, it operates a Language Technology Lab, headed by Yao Tianfang (姚天昉), specializing in Internet-based information extraction and data mining. Other labs at Shanghai Jiao Tong include Information Coding and Theory, and Trusted Digital Technology.[139]

- Gu Dawu's work in particular illustrates government sponsorship of technical work with information warfare implications, having included information security projects

[137] Southeast University, *Guanyu Yinfa "Dongnan Daxue 2010 Nian Biye Yanjiu Sheng Jiuye Banfa" He "Dongnan Daxue 2010 Jie Benke Biye Sheng Jiuye Banfa" De Tongzhi* "关于印发《东南大学2010年毕业研究生就业办法》和《东南大学2010届本科毕业生就业办法》的通知 (Notice Concerning "Job Placement for Southeast University's 2010 Graduate Students" and "Job Placement for Southeast University's 2010 Undergraduate Students")." <www.seu.edu.cn>.

[138] Beijing University of Posts and Telecommunications, "*Beijing Youdian Daxue*" (Beijing University of Posts and Telecommunications).

[139] Shanghai Jiao Tong University, "Cryptography and Information Security."

funded by the 863 national high-tech research program and by the s219 national engineering program. Gu has also been awarded a "National Defense Science and Technology Progress Award" (*guofang keji jinbu er deng jiang;* 国防科技进步二等奖).[140]

- ***We assess that some highly focused information warfare-applicable research is also being conducted in the State Secrecy Academies, established by the State Secrecy Bureau and the Ministry of Industry and Information Technology at four universities around China (Harbin Institute of Technology, Nanjing University, Sun Yat-Sen University, and Northwestern Polytechnical University).*** These four schools all have areas of specialization in information and network security, cryptography, and computer science, which we assess likely drove the government's approval for the placement of State Secrecy Academies at these institutions.

- **Northwestern Polytechnical University or NWPU** (*xibei gongye daxue;* 西北工业大学) is, like HIT, a center of both funding and expertise in a variety of information security themed projects and research. NWPU's hosting of one of four national state secrecy academies, featured academic majors in information confrontation and information security, and graduate programs in only two areas (computer engineering and information security) suggest that it is a key center of information warfare research similar to HIT. The State Secrecy Bureau's recognition of NWPU's "resources in information technology, information engineering, and network security"[141] along with the other three universities selected to host State Secrecy Academies, suggests a centralized government effort to integrate collaborative relationships with civilian academic institutions into China's technical training supporting its national information security efforts, and to use the expertise of the academic environment to groom reliable talents in the field of information security and state secrets protection.[142]

- Professor Cai Wandong (蔡皖东) of NWPU serves as the Director of the National Classified Information System Security Evaluation Center, as well as sitting as a committee expert for national-level information security project evaluations. In that capacity, Cai likely influences selections for the most sensitive information security projects funded by national-level academic grants.

- NWPU's Network and Information Security Department has been recognized at the provincial level for its expertise in network security monitoring, disaster recovery, and of particular note, a "hacker control system."[143]

[140] Shanghai Jiao Tong University, "Gu Dawu."
[141] Wang Fanhua..
[142] Ibid.
[143] Northwest Polytechnical University, "*Jisuanji Xueyuan Xueke Fangxiang Jieshao*" (Introduction to the Computer Science Department).

Chinese Telecommunications R&D—State and Commercial Cooperation Pushing Industry Growth

The volume of data consumed by the PLA as it pushes forward with informationization is vast and continues to grow, especially as it brings additional sources of intelligence collection, tactical data links, and multiple communication networks online. China's C4ISR networks require a highly advanced national telecommunications infrastructure to accommodate this dramatic volume increase. The success of informationization as a vehicle to modernize PLA C4ISR is quite literally dependent on the ability of the country's telecommunications sector to meet these demands for new systems and capabilities. The Chinese are addressing this issue with a now decade-long transformation of its telecommunications systems and by extension, the military's C4ISR infrastructure. This expansive overhaul has shifted military communications and data networks to widespread use of secure digital communications over fiber optic cable, advanced high frequency radios, microwave, and secure satellite networks.

The highly vertical integration of traditional Chinese defense industries that relied on narrow, often domestic sources of supply could not support or sustain the dynamic, highly successful IT modernization underway in the PLA. China's IT sector is most accurately considered as a largely civilian sector of China's economy but which maintains links to the PLA and to other Chinese defense industries. Rather than isolate collections of state owned IT firms as exclusively "defense" in orientation, the PLA, often operating through its extensive base of R&D institutes, alternately collaborates with China's civilian IT companies and universities or benefits as a customer of nominally civilian products and R&D. Additional government patronage of defense related IT research comes in the form of funding from national grant programs such as the 863 Program, 973 Program and 242 Program outlined above and direct funding for R&D activities.

- China maintained 3,707 research institutes nationally in all fields staffed by 32.3 million people according to 2009 statistics, the most recent year for which these figures are available. In 2010, China invested RMB411.44 billion in S&T nationally, approximately 4.58% of the overall national budget, according to the Chinese National Bureau of Statistics.[144]

This phenomenon is captured in a model first published in a 2005 RAND Corp study of the Chinese defense industry, that the authors describe as a the "digital triangle," a paradigm shift from traditional models of state owned enterprise (SOE) driving defense related R&D for

[144] PRC National Bureau of Statistics, "*Di Er Ci Quanguo Kexue Yanjiu Yu Shiyan Fazhan (R&D) Ziyuan Qingcha*" (Second National Scientific Research and Development Resource Inventory No. 3) (22 November 2010).

largely military customers, all managed centrally by a central planning entity.[145] In the digital triangle model, three components or "vertices" interact in a collaborative model in which the military or their sponsored research institutes funds the R&D activities of commercial firms such as Datang, Huawei, or ZTE and often designate them as "national champions" by the state. This designation enables them to receive priority for funding through state sponsored technology grant programs such as the 863 Program or easy access to lines of credit from state run banks.[146] The digital triangle model, the authors note, has moved the PLA away from large consortia of state-run IT enterprises operating in "stovepipe" organizational models for exclusively military customers.

In the IT sector, the government has concentrated on the indigenous development of commercially viable products rather than the acquisition of difficult to obtain foreign technology. Under the digital triangle model, PLA R&D institutes can collaborate directly with civilian universities and private commercial IT firms such as ZTE or Huawei or hundreds of smaller niche firms. Improving the fluidity of technology transfer between civilian and military users and researchers is a significant enough priority that the State Council included it as an item on China's *Medium and Long-Term S&T Program Guidelines for 2006-2020*, the strategic roadmap for national S&T development. The document references "perfecting mechanisms for combining military and civilian production and combining military capabilities in civilian capabilities."[147]

The military benefits from the access to cutting edge research that is often carried out by the commercial firms with legitimate foreign partners supplying critical technology and sometimes sharing the cost of the R&D. A secondary benefit to the PLA of this strategy is the ready access to the latest COTS telecommunications technology brought in by China's access to the foreign joint ventures and international commercial markets.[148]

The IT sector in China can be considered a hybrid defense industry, able to operate with success in commercial markets while meeting the demands of its military customers. The Chinese telecommunications market is heavily influenced by its largest domestic members—such as hardware and networking giants Huawei Shenzhen Technology Company, Zhongxing Telecom (ZTE), and Datang Telecom Technology Co., Limited. These companies and some smaller players are not always directly linked to the PLA or C4ISR modernization because of their strong domestic and international commercial orientation. The digital triangle model, however, allows them to benefit directly from a background network of state research institutes and government funding in programs that do have affiliation or sponsorship of the PLA.

---

[145] Evan S. Medeiros, Roger Cliff, Keith Crane, and James C. Mulvenon, *A New Direction for China's Defense Industry* (RAND Corp., 2005). See also James Mulvenon and Rebecca Samm Tyroler-Cooper, "China's Defense Industry on the Path of Reform" (U.S. China Economic and Security Review Commission, October 2009).

[146] Medeiros 206.

[147] "Apparent Text of PRC Medium- and Long-Term S&T Program Guidelines for 2006-2020" (Xinhua Domestic Service, 9 February 2006).

[148] Mulvenon and Samm Tyroler-Cooper 37.

China's national strategy to harness the benefits of dual use technology under a formal program, Locating Military Potential in Civilian Capabilities (*yujun yumin;* 于军于民) as part of the 10th Five Year Plan (2000-2005), later refined by Hu Jintao into "civil-military fusion" (*junmin ronghe;* 军民融合) during the 11th Five Year Plan, has allowed the civilian sectors of the economy to have greater access to PLA procurement and fuel the military modernization process.[149] As Chinese defense budgets have continued to increase, commercial firms have had greater incentive to get involved in military procurement and a GAD survey of Chinese civilian high tech firms discovered that over 90% of the IT firms surveyed in 2005 were already involved with military acquisition and production, according to PLA media reporting cited in Western analysis of these programs.[150]

The state supervises Chinese defense industries via the Ministry of Industry and Information Technology (MIIT) a relatively new "super-ministry" created in 2008 during the Eleventh National People's Congress. The creation of MIIT consolidated the Ministry of Information Industry with three other State Council departments, including the State Administration of Science, Technology, and Industry for National Defense (SASTIND), formerly the Commission of Science, Technology and Industry for National Defense, (COSTIND).[151] While these bureaucratic reforms were taking place, the PRC State Council, China's highest executive branch authority, also created the Civil Military Integration Promotion Department (CMIPD). Subordinate to MIIT, it is chartered to work with SASTIND on policy development for dual use technologies, promoting tighter integration of civilian and military industries and oversight of the defense grant programs that support much of the defense-related R&D in China's civilian universities.[152]

- In October 2011, CMIPD sponsored a provincial level dual use technology "matchmaking" conference (*junmin liangyong jishu hezuo duijie hui;* 军民两用技术合作对接会) in Shaoxing, Zhejiang Province that brought together PLA representatives, 150 commercial businesses, seven universities, and 100 research institutes, according to information on the CMIPD website.[153] The Zhejiang conference featured exhibits and discussions on over 1000 dual use projects.

- MIIT and CMIPD regularly sponsor similar events elsewhere in China since 2008, suggesting that CMIPD and the PLA are taking a more active and direct role in pairing priority needs with commercial sector resources.[154]

[149] Mulvenon and Tyroler-Cooper; see also Micah Springut, Steven Schlaikjer, and David Chen, "China's Program for Science and Technology Modernization: Implications for American Competitiveness" (U.S.-China Economic and Security Review Commission, January 2011): 119.
[150] Springut 119.
[151] Ibid 7.
[152] PRC Ministry of Industry and Information Technology, "Military-Civilian Promotion Division."
[153] PRC Ministry of Industry and Information Technology, "*Zhejiang Sheng Chenggong Juban Junmin Liangyong Jishu Hezuo Duijie Hui*" (Zhejiang Province Successfully Holds Dual-Use Technology Cooperation Matchmaking) (17 October 2011).

[154] "*Shi Nian Gao Jiaohui Junmin Keji Jie Shuoguo*" (10th Annual Exhibition: Dual-Use Science and Technology) (Chongqing Civilization Network, 8 July 2010).

Huawei, ZTE, and Datang are the leading telecommunications equipment manufacturers in China and among the top five in the world by volume of sales, accounting for the highest market share of 3G network construction. They have distinct product and service offerings, different origins, and unique strategies for competing in both domestic and international markets. Yet they are each deeply integrated into the digital triangle model and actively work with the PRC government as both vendors and research collaborators.

Zhongxing Telecom Technology Corp (ZTE, *zhongxing tongxun gufen youxian gongsi;* 中兴通讯股份有限公司)**,** is a multinational telecommunications equipment and systems company headquartered in Shenzhen, China. ZTE is currently the second-largest Chinese telecommunications equipment maker (after Huawei) and the world's fifth-largest mobile phone manufacturer. The majority of ZTE's customers are outside of China as a part of the company's deliberate strategy to focus on gaining market share with largely mobile network operators in developing countries. ZTE, however, has succeeded in penetrating markets in more developed countries as well. Founded in 1985 as a spin-off of the 691 Factory under the China Aerospace Industry Corporation, ZTE is no longer a state-owned enterprise but it does maintain research relationships with a variety of Chinese universities and military institutes as a collaborating research partner.

- The company is focused heavily on capturing market share internationally and earned over half of its revenue from overseas markets, with North American and European generated revenue growing by 50% in 2010 to become the largest proportion of ZTE's overseas revenue, according to the company's 2010 annual report.[155]

- ZTE has between 60,000 and possibly as many as 95,000 employees, maintains 107 representative offices around the world, and 15 research labs throughout North America, Europe, and Asia with a dedicated research staff of approximately 15,000 staff, according to company supplied data on its Chinese language website.[156]

- The UK's Vodafone, Canadian Telus and Public Mobile, and France Telecom have all purchased equipment from ZTE and many Chinese companies are also ZTE customers, including China Netcom, China Mobile, China Satcom, China Telecom, and China Unicom.

- ZTE's hardware product line includes the production of program-controlled switching systems, multimedia communications systems, communications transmission systems, production systems for mobile communications equipment, satellite communications, microwave communications equipment, pagers, computer hardware and software, closed-circuit television, microwave communications, and automatic control signals.

[155] ZTE Corporation Annual Report 2010 (*Zhongxing Tongxun Gufen Youxian Gongsi Niandu Baogao* 中興通訊股份有限公司年度報告2010), p. 142.

[156] <http://www.zteusa.com/about/press/news/>. Note, these statistics do not appear on the company's English language website.

- ZTE has provided wired and wireless communications networks in over 30 countries for projects that include railways, subway systems, urban rail transit, highways, factories, mines, ports, airports.[157]

ZTE devotes considerable internal resources to R&D, with as much as 34 percent of its workforce and 10 percent of its revenue dedicated to innovation of new products and services. This investment, in conjunction with its deep accessibility to the international market, enables ZTE to capture foreign market share while acting as a conduit back into China for foreign COTS technology.

- Company statistics note that they are the second highest filer of international patent applications and currently hold 1,863 international patents, according to information on the Chinese language version of the company's website.[158]

- In 2010, Hu Jintao attended the Emerging Strategic Industries Exhibition (*zhanluexing xinxing chanye zhan* 战略性新兴产业展) in Shenzhen where he met briefly with ZTE representatives to discuss the importance of TD-LTE development (China's domestically-developed next generation 4G wireless network standard), suggesting that the PRC political leadership has placed particular strategic importance on the standard for Chinese growth and recognizes ZTE's importance in its development. TD-LTE is currently deployed only to domestic Chinese cities and is being tested in Taiwan.[159] It is supported by international vendors Nokia and Ericsson.[160]

- The diversity of the company's telecommunications hardware products has also enabled it to acquire contracts in dozens of foreign countries where ZTE's ability to customize network designs with greater flexibility and lower costs than its competitors has won it market share.

ZTE maintains a diverse relationship with the PLA that encompasses collaborative research with military and civilian universities, including satellite navigation, data link jamming techniques, training of active duty PLA personnel, and as a regular exhibitor and presenter at PLA sponsored defense industry expositions. ZTE has, according to one Western researcher, been a prime supplier of customized telecommunications services and hardware to the PLA, including trunk-like optical network systems.[161]

[157] http://www.zteusa.com/about/press/news.
[158] Zhongxing Telecom, "About ZTE." <www.zte.com.cn>. This statistic is not published on the nominally identical English language site.
[159] Mobile 4G: China Mobile Rolling Out TD-LTE Trials." *GoMo News* 4 January 2011. <http://www.gomonews.com/mobile-4g-china-mobile-rolling-out-td-lte-trials/>.
[160] "Nokia Booklet 3G *Bianzhong Da Shang* TD-LTE *Yu Beijing Xianshen, Kexi Zhi Shi Ceshi Ji*" (Nokia Booklet 3G TD-LET Variant Appears in Beijing; Unfortunately, It Is Only a Test Device), (Engadget, 27 September 2011).
[161] Tai Ming Cheung, *Fortifying China: The Struggle to Build a Modern Defense Economy* (Cornell University Press, 2009): 219-220 and 222.

— Personnel from ZTE's Xi'an Institute have exhibited at, and participated in, technical presentations at the 2009 Microwave Industry Exhibition in Xi'an in May 2009 and the Shanghai Military and Commercial Technology and Electronic System Exhibition in 2007. The marketing materials for the Microwave conference indicate the event featured research and products from the ZTE Xi'an Institute, PLA Second Artillery Engineering College, CETC 20th Research Institute, CETC 39th Research Institute, the 206 Institute of China North Industries Corporation (NORINCO), and the Xi'an Research Institute of Huawei Technologies.[162]

— ZTE, along with other major civilian telecommunications companies such as Huawei and China Mobile, is a regular exhibitor at a civilian-military dual use tech-expo sponsored jointly by the PLA GSD, GAD Department of Electronic and Information Infrastructure, MIIT, and the Chinese Academy of Sciences, according to publicly available conference materials.[163]

— ZTE researchers were also leading presenters and exhibitors at a 2009 PLA sponsored defense industry conference on RFID technology held at the Beijing Fentai Armored Force Engineering Institute. Industry online media reporting indicates that PLA attendees included GAD and General Logistics Department (GLD) personnel who are responsible for purchasing and acquisition. ZTE presenters highlighted various military logistics applications of their RFID technologies, but specifically focused on the information security aspects of ZTE's RFID products for static and dynamic key authentication.[164]

— ZTE's UHF RFID tags also appear on a list of security products approved by the PLA's Military Security and Protection Center for use on government and military networks. The Center is a GSD entity established in May 2008 to evaluate physical and information security products and certify them for use on PLA networks, according to information provided on the Center's website.[165]

— A ZTE researcher affiliated with the company's Xi'an Research Institute co-authored a 2007 study that analyzed the anti-jamming characteristics of the U.S. Navy's JTIDS data link system. Together with a researcher from the PLA Air Force Engineering Institute, the authors analyzed methods and waveforms that may successfully jam a

[162] Interference Technology, "2009 Microwave Industry Exhibition Invitation" (17 February 2009).
[163] See conference announcement at: http://wwwz606.com/news/view.php?id=293; materials note that is the 5th annual dual use technology event and is open to U.S. and other international companies to exhibit. The roster of attendees notes the presence of Motorola, Cisco, Ford, Whirlpool, as well as European and Japanese companies.
[164] "ZTE Vision for a Comprehensive RFID Solution Unveiled" (*Zhongxing RFID Keshihua Zhengti Jiejue Fang'an Liangxiang;* 中兴RFID可视化整体解决方案亮相), 29 March 2009.
<http://www.99rfid.com/AnLi/NewsList.Asp?DonforType=administrator200849173018>.
[165] "*Junyong Anquan jishu Fangfan Chanpin Di Si Pi Yi Renzheng Chenggong*" (Fourth Installment of Military Security Products Certified). 25 January 2010.

JTIDS system, suggesting that ZTE personnel are supporting offensive electronic warfare research with PLA academic and operational personnel.[166]

In September 2008, ZTE Corporation signed an agreement to invest more than six billion yuan to build an R&D and production base in the Xi'an High Technology Industries Development Zone (XHTDZ). The project will focus on developing and producing future 3.5G and 4G communication products, according to information originally published on the Zone's website. The zone is home to a concentration of some of China's most innovative high technology communications firms, universities, and research institutes, receiving significant outside investment, which has helped drive the growth of both the national-level and local firms based in the area.[167]

In October 2009, ZTE opened a 4G, or Long Term Evolution (LTE), laboratory in Richardson, Texas as part of its North American subsidiary, ZTE USA in a bid to use the facility to showcase the company's dual-mode CDMA (code division multiplex access) and LTE platform. LTE is a fourth-generation wireless data standard in the GSM wireless family that has also been adopted by most major U.S. telecommunications carriers.[168] ZTE is using the Richardson, TX lab to develop this dual-mode CDMA/LTE platform as the product basis for expanding their presence in the U.S. market, according to statements by ZTE USA's president Jiang Xiangyang.

- ZTE USA primarily offers wireless handset and networking solutions in the United States. ZTE highlights in their marketing materials that they are researching the means to produce dual mode devices incorporating both LTE and the Global System for Mobile Communications (GSM). The GSM standard continues to be used by majority of carriers worldwide, including major U.S. carriers. ZTE's incorporation of GSM into dual-mode devices reflects intent to continue their expansion into international markets.

- Increasing pressure to lower costs associated with wireless networking in the United States is pushing many vendors to begin considering alternative, often foreign, sources of both hardware and services, making Chinese options like ZTE and new standards advocated by Chinese providers and government such as Worldwide Interoperability for Microwave Access 21 (WiMAX) and LTE standards begin to look much more attractive.[169]

---

[166] Duan Yajun, Wu Chang, and Li Chengen, "Analysis of Anti-Jamming Performance of JTIDS System" (*Zhuangbei Zhihui Jishu Xueyuan Xuebao* (Journal of the Academy of Equipment Command and Technology), October 2007): 81.

[167] See information provided on www.xdz.com.cn.

[168] LTE (Long Term Evolution) refers to the new air interface that will be delivered by 3GPP, the 3rd Generation Partnership Project, in its Release 8 Specification set. LTE will provide users with a personal media experience similar to that of fixed line broadband both in terms of bandwidth and latency, meaning applications that can be delivered today on fixed line will soon be available over the air and with full mobility with LTE. See "AT&T to Deliver 3G Mobile Broadband Speed Boost," AT&T Press Release, May 27, 2009. <http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=26835&mapcode=>.

[169] "The National Security Implications of Investments and Products from the People's Republic of China In The Telecommunications Sector" (U.S.-China Economic and Security Review Commission, January 2011): 12.

Huawei Shenzhen Technology Company Ltd*:* Huawei (*Shenzhen huawei jishu youxian gongsi* 深圳华为技术有限公司) was founded in 1988 by Ren Zhengfei, the former director of the GSD Information Engineering Academy, the PLA's primary center for telecommunications research. Currently the second largest manufacturer of telecommunications equipment in the world, specializing in the R&D, production, and marketing of communications equipment and the implementation of customized network solutions for telecommunications carriers, it is also one of the most widely known Chinese companies both for its success in winning international market share. The firm's name recognition, however, is also the result of its many blocked acquisition attempts of foreign firms based on national security concerns over Huawei's perceived relationship with the PRC government and the PLA.

Beijing clearly views Huawei as a strategically important company for the impact on China's IT sector and its international competitiveness. Western analyses of the company point out that Beijing formally designated Huawei a "national champion" company, which is a formal designation developed by the State Council's State Owned Assets Supervision and Administration Commission (SASAC) to identify state-owned enterprises which are considered to have strategic value to China's national security.[170] If this assertion is accurate, then it reflects just how strongly the PRC leadership feels about Huawei's value to China's IT sector and how its broader capabilities drive innovation to the PLA and brings innovation into China.[171] Very few Chinese companies have played such an influential role in integrating the Chinese IT sectors into the global marketplace allowing Chinese companies to operate internationally as competitors rather than simply as assemblers of foreign products. The access to cutting edge international COTS technologies in turn has created numerous "spin-on" opportunities for civilian companies to develop dual use products that meet the PLA's requirements.[172] This dynamic has allowed Huawei and many other smaller niche firms to become sources of advanced technology for the PLA.

The promulgation of the "Tender Law," further streamlined the methods by which Chinese companies compete for PLA business. Though primarily intended to improve the process by which the PLA awards contracts to commercial firms, the law also encouraged selected companies to rationalize product offerings, improve performance, and increase operating efficiency. These improvements will benefit the PLA over the longer term as they have domestic access to higher quality microelectronics and other technologies. A 2009 PLA National Defense University book highlights the effect of the law with regard to sensitive high performance integrated circuits:

[170] Evan Medeiros et al., *A New Direction for China's Defense Industry* (Arlington, VA: RAND Corporation, 2005), pp. 217-218

[171] SASAC's official website, however, does not indicate that Huawei formally holds this title, which conveys special privilege on the enterprise to obtain lines of credit, funding, and policy related preferential treatment. SASAC is the PRC entity responsible for making this designation. See http://www.sasac.gov.cn.

[172] An example of classic "spin-off" models of technology transfer would be the United States early space program and defense-related satellite and communications technologies in which advanced technologies developed with strictly government resources and often as classified programs eventually found extensive application in the civilian sector.

> The state has already made the Tender Law, which proposes the implementation of a public tender system for parts and components projects while the laws and regulations governing the production of military products are being observed, encourage solid domestic manufacturing units to participate in fair competition and encourage joint research and development. For example, institutes of higher learning and suppliers can use their own strengths to jointly research and develop new products. Several years ago, in order to develop military integrated circuits, we chose some private companies to research and develop military products. For example, they include such manufacturing units as Shenzhen City Guowei Electronics Co., Limited, Chengdu Huawei Microelectronics Co., Limited, National University of Defense Technology, and Fudan University Microelectronics Co., Limited. They have developed a number of parts and components whose export was banned by other countries and many of which are now in mass production for bulk orders. This has greatly improved the level of China's microelectronics industry. That private companies participate in competition can promote suppliers of military parts and components to actively reform, increase the variety of products that are available to consumers, improve the performance, quality and reliability of their products.[173]

Huawei's involvement with PLA research and development either directly as a vendor or indirectly as a research collaborator with various PLA affiliated organizations or universities all weaken claims by Huawei's leadership that it maintains no ties with the Chinese government or the military***. The combination of recent infusions of cash, regular appearances at PLA defense industry events, and working relationship with various government research institutes on projects with dual use applications suggests that an ongoing relationship between Huawei and the Chinese military and Chinese political leadership may exist.***

- An uncorroborated October 2010 report in the pro-Beijing Chinese newspaper *Xinjing Bao* stated that Huawei Chairwoman Sun Yafang worked for the Communications Department of the PRC Ministry of State Security for an unspecified period of time before joining Huawei. According to an undated report on Hong Kong-managed news site *Feng Huang Wang,* Sun used her MSS connections to help Huawei through financial difficulties in 1987 as the company was entering its early years of development. An official description of Huawei's directors posted to the company's website in April, 2011 contained no mention of Sun's past MSS affiliation and Sun's past government and intelligence affiliations remain unconfirmed.[174]

    - An April 2011 article in a Chinese financial daily covering securities issues reported that the PRC government gave Huawei RMB 250 million (U.S.$36.8 million) and

[173] Li Yan and Wang Jinfa, *Junmin Ronghe Da Zhanlue* (Military-Civilian Fusion Grand Strategy) (National Defense University Press, October 2009).

[174] Open Source Center, "Huawei Annual Report Details Directors, Supervisory Board for First Time" (5 October 2011). Rumors of Sun's past MSS employment are not new, and in fact go back as far as March 2005. See for example diviner, "*Tongxin Rensheng–Huawei Jishu Youxian Gongsi Dongshi Zhang Sun Yafang Jieshao"* (Communications Lifestyle–Introduction to Huawei Technology Co., Ltd. Chairwoman Sun Yafang) (China Communications Network, March 9, 2005).

RMB 430 million (U.S.$63.2 million) in 2009 and 2010, respectively for "domestic development, innovation, and research."[175]

- The company also received government funding amounting to RMB 328 million (U.S.$48.2 million) and RMB 545 million (U.S.$80 million) in 2009 and 2010, respectively for "completing certain research projects" according to additional uncorroborated PRC press reporting.[176]

Huawei may also be involved in supporting PLA active duty units with short term training in networking design and construction, possibly supporting the military region command system with technical experts and "train-the-trainer" programs.

- As early as 2005, official PLA media sources in the Guangzhou MR, which includes the Shenzhen area where Huawei is headquartered, reported on a PLA program to train members of its communications units at area PLA universities and through formal exchange programs with Huawei that brought company personnel to the PLA units and allowed the soldiers to spend time in technical training at company locations.

- Huawei, like ZTE, exhibited at an April 2010 PLA civilian-military dual use technology exposition sponsored by the PLA MIIT, and the Chinese Academy of Sciences, according to conference materials.[177]

- Huawei maintains a formal funding mechanism called the "Huawei Technology Fund" (*huawei keji jijin;* 华为科技基金) that has supported research at both civilian and PLA universities in eight defined areas of inquiry that include wireless communication, optical communication technology, broadband technology, computer processing and application specific integrated circuit (ASIC) technology, and communication circuits and system research, according to a review of the grant application and requirements; many of the grant recipients have also received National 863 and 242 grants, suggesting they are involved in defense or national security related work.[178]

Datang Telecommunications Science and Technology Co., Ltd. (*datang dianxin;* 大唐电信), headquartered in Beijing, is a PRC state-owned telecommunications equipment

[175] Chen Dingrong and Dai Yu, "Setting Off a New Upsurge in Training With Preparation for Military Struggle in Mind" (*Guangzhou Zhanshi Bao*, 30 September 2005): 1.
[176] *Zhengquan Ribao.*
[177] See conference announcement at: http://wwwz606.com/news/view.php?id=293.
[178] See for example the faculty profile for Prof Chen Enhong, China University of Science and Technology. <http://dm.ustc.edu.cn>, director of the Laboratory of Semantic Computing and Data Mining, and also Prof Xu Chunxiang University of Electronic Science and Technology of China, School of Computer Science and Engineering. <http://www.ccse.uestc.edu.cn/teacher/teacher.aspx?id=11>; the grant application is available from various university websites, see for example: Xian Jiao Tong University Science and Technology Department, http://std.xjtu.edu.cn.

manufacturer, vendor, and integrator specializing in hardware and cabling for switching, optical, and large-scale wireless mobile communications networks. Nationally recognized as a "National Innovation-Oriented Enterprise," Datang is often listed as the third largest telecommunications vendor in China, after Huawei and ZTE, and serves a mostly domestic Chinese telecommunications market. Datang has been the beneficiary of considerable state funding for research and development, especially involving the development of technologies integrating the Chinese domestic Time Division-Synchronous Code Division Multiple Access (TD-SCDMA) 3G wireless standard, which it created.[179]

Datang was founded in 1998 by an investment group including the Chinese Academy of Telecommunications Technologies (CATT) and the 10th Research Institute, both under the Ministry of Information Industry (later known as the Ministry of Industry and Information Technology).[180] Datang's continued status as a state-owned enterprise (SOE) guarantees it a level of support from PRC government entities not shared by its peers Huawei and ZTE, while possibly hindering its ability to expand into global markets and to bring commercial products to even the domestic PRC market.[181] Perhaps in an effort to reduce its dependence on state support, Datang has recently opened collaborative research and development relationships with international partners such as Ericsson and Agilent to expand global integration of the TD-SCDMA standard and to develop new technologies and standards promoting the Chinese national TD-LTE transitional 4G wireless standard for the PRC and other markets.[182] As an SOE supervised by SASAC, Datang benefits from close government relationships for which Huawei and ZTE may sometimes find themselves ineligible as private companies.[183]

- Datang has long been focused primarily on domestic Chinese markets, with some export to global markets; however, recent statements by its Swedish venture partner, telecommunications manufacturer Ericsson, suggest that Datang will expand the promotion of its TD-SCDMA standard globally. Datang already exports hardware products to a North American market.[184]

- Datang subsidiary, Datang Software Technologies, Ltd., a provider of telecommunications network management systems, operation supporting system, business supporting

[179] Chen Shanzhi, "Datang Telecom Technology & Industry Group" (July 2009); Datang Telecom, "Datang Telecom Technology Co., Ltd."; Datang Telecom, "DATANG TELECOM TECHNOLOGY & INDUSTRY GROUP," <http://www.datanggroup.cn/en/index.aspx>; "Datang Telecom Technology Co Ltd (600198.SS) Company Profile." Reuters; and Tsai, Ching-Jung and Wang, Jenn-hwang, "How China Institutional Changes Influence Industry Development? The Case of TD-SCDMA Industrialization" (Druid Society, June 2011).

[180] Jintong Lin, Xiongjian Liang, Yan Wan. Telecommunications in China: Development and Prospects. ©2001, NOVA Science Publishers, Inc. pp.95-100.

[181] Tsai, et al.

[182] "Agilent Technologies and Datang Telecom Group Establish Joint Research Lab to Accelerate Development of Next-Generation Wireless Technology in China" (BusinessWire, 13 October 2011).

[183] PRC State Council, "*Gongye He Xinxi Hua Bu Zhuyao Zhize Nei She Jigou He Renyuan Bianzhi Guiding Yinfa*" (Issuance Concerning the Major Internal Organization and Staffing Responsibilities of the Ministry of Industry and Information Technology) (11 July 2008).

[184] "Strategic cooperation with Datang for mobile technology development in China" (Ericsson, 20 April 2010); "Datang Telecom Technology Co., Ltd." (Bizearch.com, viewed November 2011).

systems, e-government, enterprise wireless access platform, and wireless solutions for small and medium business, has counted among its customers Cisco, Dell, HP, IBM, Oracle, and Sun in the fields of mainframe, server, storage, and data warehouse middleware.[185]

- Datang has recently entered into collaborative research and development relationships with international telecommunications partners to expand implementation of the TD-SCDMA standard and to develop newer technologies including those integrating the 4G TD-LTE standard.
    - In April, 2010 Swedish telecommunications and data communications provider Ericsson announced a strategic cooperative agreement with Datang to develop technologies for both Chinese and global markets. As part of this agreement, Ericsson announced its intention to integrate the TD-SCDMA standard into its 3G mobile communications products.[186]
    - In October 2011, Datang entered an agreement with multinational electronic test equipment manufacturer Agilent to establish a joint research and development laboratory to develop new technologies, test standards, and promote TD-LTE-Advanced technologies.[187]
    - Datang has engaged in other foreign cooperative relationships with Siemens, Compaq, and Nortel.[188]
- Datang has also long been involved in cooperative research ventures with Chinese high-tech universities, including Peking University, Southeast University, Tsinghua University, Xi'an Jiao Tong University, Beijing University of Posts and Telecommunications, and Shanghai Jiao Tong University. These engagements frequently focus on wireless communications.[189]
- Datang's manufacturing offerings consist of radio access stations, broadband access architecture, processor chipsets, terminals, and emergency communication systems as well as voice over IP gateways.

[185] sourcexperts.com, "Datang Software Technologies, Ltd." (19 January 2005). Oracle, "Datang Software Technologies Certifies Their Telecom Network Resource Management System on Oracle Database 11g and Oracle Real Application Clusters" (May 2009).
[186] Ericsson, "Strategic cooperation with Datang for mobile technology development in China" (20 April 2010).
[187] "Agilent Technologies and Datang Telecom Group Establish Joint Research Lab to Accelerate Development of Next-Generation Wireless Technology in China" (BusinessWire, 13 October 2011).
[188] Medeiros 213.
[189] Shanghai Jiao Tong University, "*Datang Dianxin Jituan Lai Wo Xiao Jinxing Xiao Qi Hezuo Diaoyan*" (Datang Telecom Group to Visit, Will Conduct Academic-Commercial Cooperative Research) (8 November 2010).

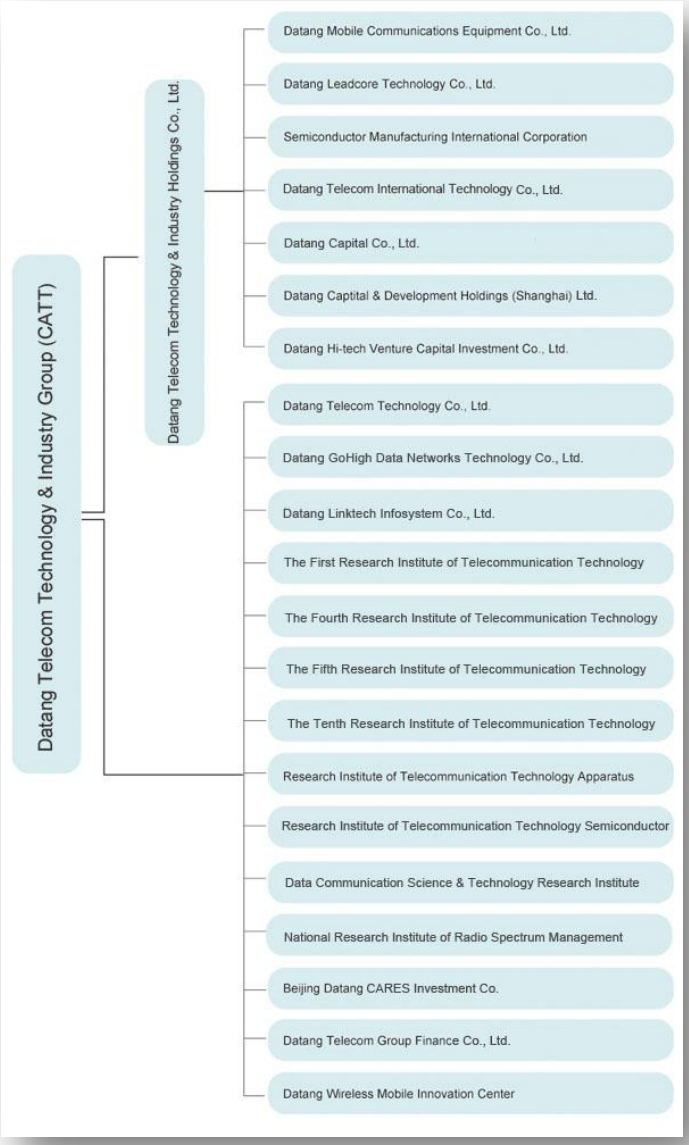

Figure 3: Datang organization chart. Source is Datang Telecom, "Organization Structure," <http://en.datanggroup.cn/templates/00Content%20Page/index.aspx?nodeid=13>

Datang's parent organization, Datang Telecom Technology and Industry Group, operates a handful of numbered research institutes inherited from CATT, with which it effectively merged in 1999: namely, the First, Fourth, Fifth, and Tenth Research Institutes of Telecommunications Technology.[190] Datang enjoys a close relationship with MIIT by virtue of its evolution from the CATT. The division of labor between Datang and MIIT concerning the administration of these research institutes merits further study.

[190] Jintong Lin, Xiongjian Liang, Yan Wan. Telecommunications in China: development and prospects. ©2001, NOVA Science Publishers, Inc. pp.95-100. The Datang Group also operates four research institutes focusing on technical areas of telecommunications: the Research Institutes of Telecommunications Technology Apparatus, Telecommunications Technology Semiconductor, Data Communication Science and Technology, and Radio Spectrum Management.

The First Research Institute of Telecommunications Technology (*dianxin kexue jishu di yi yanjiu suo;* 电信科学技术第一研究所), located in Shanghai, specializes in research and development of emergency services and social services information systems, satellite communications and wireless communications systems, mobile communications network optimization, and communications equipment quality supervision and inspection.[191]

The Fourth Research Institute of Telecommunications Technology (*dianxin kexue jishu di si yanjiu suo;* 电信科学技术第四研究所), located in Xi'an, specializes in microwave wireless communications and the quality supervision and inspection of wireless communication products. As the sole SOE specializing in microwave wireless communications, the Fourth Institute maintains "close" but unspecified relations with the PLA, including construction of military communications infrastructure.[192] The Fourth Research Institute developed the M4000 microwave wireless mobile communication system, fielded to various government agencies according to the institute's website, including counter-terrorism operations in China's northwest Xinjiang Province, and military command vehicles.[193]

The Fifth Research Institute of Telecommunications Technology (*dianxin kexue jishu di wu yanjiu suo;* 电信科学技术第五研究所), located in Chengdu, specializes in analog, digital, fiber-optic communication systems technology research and product development. Participant in numerous 863 Program projects, according to the Fifth Research Institute's website, it is currently conducting research and development in cable testing techniques, special optical transmission, and access technologies, working with the Ministry of Science and unspecified military projects in its product development.[194]

The Tenth Research Institute of Telecommunications Technology (*dianxin kexue jishu di shi yanjiu suo* 电信科学技术第十研究所), also known as the Datang Telecommunications Group (Xi'an) Research Center (*datang dianxin jituan (xi'an) yanjiu zhongxin* 大唐电信集团(西安)研究中心), located in Xi'an, specializes in telephone exchange and public telegraph switching for the Directorate General of Telecommunications, computer communications and network information security, multimedia, communications, software and mechanical processing for high-tech enterprises.[195] ***Publicly accessible information indicates that Datang enjoys a continuing relationship with the PLA as a supplier of high-tech communications equipment and services, and possibly as a joint research and development partner on specific projects. The certification of Datang's 10th***

[191] Datang Telecom. "*Dianxin Kexue Jishu Di Yi Yanjiu Suo*" (First Research Institute of Telecommunications Technology).
[192] Fourth Research Institute, "*Yewu Jieshao*" (Description of Products).
[193] Fourth Research Institute, "*Dianxin Kexue Jishu Di Si Yanjiu Suo*" (Fourth Research Institute of Telecommunications Technology); Fourth Research Institute, "*Kuandai Wuxian Yidong Duomeiti Tongxin Xitong*" (M4000 Broadband Wireless Mobile Multimedia Communication System).
[194] Fifth Research Institute. "*Wu Suo Jieshao*" (About the Fifth Institute).
[195] Datang Telecom, "*Datang Dianxin Keji Chanye Jituan*" (Datang Telecom Technology & Industry Group); East Fortune. "Telecommunications Science and Technology Institute About _ tenth Datang Telecom."

Telecommunications Research Institute to handle classified high-tech projects, together with its focus on computer communications and network information security, suggests that it may collaborate with PLA units or state security offices on classified computer network and information security programs.

Some unofficial sources claim that the Tenth Research Institute is possibly involved in the development of clandestine monitoring systems, including fixed telephone line monitoring systems, and may carry out work for "secret" customers. Supporting this, PRC stock market analyses report that the Tenth Institute is engaged in network information security projects and in 2005 passed military-standard quality management system certification; received accreditation as a secret weapons research and production unit; achieved military electronic equipment research and production licenses; and achieved a grade of A for national classified computer information systems integration. In 2005 and 2008 respectively, according to the investment report, it was accepted on the development team for China's Shenzhou VI and Shenzhou VII manned spaceflight programs.[196] Other sources, also unverified, noted as of March 2010 that the Tenth Research Institute developed much of the technology that later was used by Huawei; and that the Institute suffers from harsh management and low staff morale.[197] Datang Telecom's Tenth Research Institute of Telecommunications Technology should not be confused with its Tenth Electronic Institute (*dianzi shi suo;* 电子十所) located Chengdu, Sichuan Province.[198] In 2008, the National Development and Reform Commission announced for unspecified reasons the revocation of certification for the Tenth Research Institute's Telecommunications Switching Systems and Software Support National Engineering Research Center.[199]

[196] Guba Eastmoney, "Profile of MIIT 10th Research Institute," <http://guba.eastmoney.com/look,600198,1009170152.html>
[197] Tianya BBS. "*[Xi'an] Xinren Qiuzhu, Guanyu Dianxin Kexue Jishu Di Shi Yanjiu Suo (Youdian Shi Suo)*" ([Xi'an] Newbie help request about MIIT 10th Research Institute (Posts and Telecoms 10th Institute). (1 March 2010).
[198] Datang Telecom, "Tenth Institute of Electronics."
[199] PRC National Development and Reform Commission, "*Gonggao*" (Notice).

U.S. Telecommunications Supply Chain Vulnerabilities

Supply Chain Risk Management (SCRM) is one of the twelve critical infrastructure protection priorities outlined in the White House's 2009 Comprehensive National Cybersecurity Initiative (CNCI). Although in recent years governments have begun to acknowledge the importance of supply chain protection and the problem has received high-level government attention in the United States, the complexity and global distribution of modern supply chain systems creates significant challenges for the effective mitigation of supply chain risks. The supply chain for microelectronics and telecommunications-related hardware in particular is extremely diffuse, complex, and globally dispersed, making it difficult for U.S. firms to verify the trust and authenticity of the electronic equipment they purchase. The primary threat to supply chain integrity currently appears to be criminal: profit-driven attempts to substitute authentic components with cheaply-produced, unlicensed copies of branded products. However, governments and private firms alike are increasingly concerned about the potential for state-sponsored attempts to corrupt supply chains to gain access to sensitive networks and communications, or to create the ability to control or debilitate critical systems during a time of crisis by way of vulnerabilities engineered into the integrated circuits of essential network components. Vectors into the telecommunications supply chain include both upstream, manufacturing channels and downstream, distribution channels. Each vector presents distinctive opportunities and distinctive operational costs to would-be criminals, spies, and attackers.[200]

The supply chain and fabrication process for network routers and their component integrated circuits (IC) offer a representative example of the issues and potential vulnerabilities faced broadly in the telecommunications and microelectronics hardware sectors. A review of the semiconductor industry, the router supply chain, upstream and downstream compromise opportunities, and operational challenges presented to the potential intruder highlights threat vectors, possible motives of state-sponsored adversaries seeking to penetrate or corrupt a supply chain, and potential obstacles these adversaries may face in attempting to operationalize such attempts.

Most major telecommunications and network hardware manufacturers have become largely integrators of complex systems, rather than actual manufacturers, handling the process from design conceptualization to production of sub-components to final assembly of the finished appliance by outsourcing the vast majority of these tasks to subcontractors, generic parts suppliers and their upstream supply chains. The widely-dispersed supply chain of key components may provide an intruder with opportunities to manipulate those components or penetrate the distribution chain with counterfeit products. Previous U.S. Government studies of microelectronics supply chain vulnerabilities have identified potential problems with both

[200] *Supply Chain Risk Management (SCRM).* (Information Technology Lab, National Institute of Standards and Technology, 25 January 2012); McFadden, Frank E. and Richard D. Arnold, "Supply Chain Risk Mitigation for IT Electronics," *2010 IEEE Conference on Technologies for Homeland Security* (IEEE, 2010): 49-55; Customs and Border Patrol Office of International Trade, *Publication # 0153-0112, Intellectual Property Rights Fiscal Year 2011 Seizure Statistics 2011* (U.S. Customs and Border Protection, 2012).

trust verification and the uninterrupted availability of supplies. The U.S. Department of Defense (DoD) procures its microelectronics and telecommunications hardware largely from commercial vendors, most of whom use complex, geographically dispersed supply chains, creating a vulnerability of potential insertions of malicious hardware or embedded software on the hardware components.[201]

Independent examination of a common network router conducted for this study revealed dozens of finished semiconductors from sixteen manufacturers assembled into a single product. Many of the semiconductor manufacturers subcontract all or part of the actual fabrication to other companies. Identifying the multiple layers of subcontractors and suppliers contributing to the design or fabrication of a specific chip is difficult; tracing all of the contributors for a complete integrated circuit is even more so. To ensure the identity of all suppliers to a given production run of a chip or IC are known in advance, the router vendor must negotiate specific terms with every supplier specifying the nature of the facilities and subcontractors who will contribute to the production. Sub-contractors must in turn be compelled to do the same with their suppliers, and the end to end process would need to be verified through inspections. In some cases this is done, but this approach is cost prohibitive on a large scale and for every production run.

Manufacturer	Headquarters Location	Semiconductor Fabrication and Assembly*
Fairchild	USA	China, South Korea, Malaysia, Philippines, United States
Fujitsu	Japan	China, Japan, United States
GSI Technology	USA	Taiwan
IBM	USA	Canada, Japan, United States
IDT	USA	Taiwan, United States
Intel	USA	China, Germany, Ireland, Israel, United States
Xicor (now Intersil)	USA	China, Netherlands, United States
Lattice	USA	China, Japan, South Korea, Malaysia, Philippines, Taiwan
Motorola	USA	Mexico, Malaysia
National Semiconductor	USA	Malaysia, United Kingdom, United States
NEC	Japan	China, Japan

[201] *Defense Science Board Task Force on High Performance Microchip Supply* (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005): 22-24, 35-38.

Pericom Semiconductor	USA	China, Taiwan
Pulse Electronics	USA	China
Samsung	Republic of Korea	China, South Korea, United States
STMicroelectronics	Switzerland	China, France, Italy, Morocco, Malta, Malaysia, Philippines, Singapore
Texas Instruments	USA	China, Germany, Japan, United States
		* Fabrication and packaging/assembly partner locations, where applicable

Figure 5: Sample list of network routing/switching appliance semiconductor component manufacturers

Within the semiconductor industry, pressures for efficiency, volume, and profitability have created a globally distributed foundry model, with dedicated "merchant" or "pure play" foundries that only produce chips to specifications designed by other firms and do not market their products directly. These products are then used elsewhere as part of the final design in more complex integrated circuits.[202] Many major chip firms that once maintained in-house design teams and their own proprietary foundries, a class of company referred to as Integrated Device Manufacturers (IDM),[203] have begun outsourcing steps in the process and no longer manufacture chips, but only assemble or re-brand them as they face increasing competition from smaller, more specialized design or fabrication firms. Specialized merchant foundries now represent 88% of the market, and industry analysts expect this to grow as IDMs scale back investments in new fabrication facilities.

This trend toward outsourcing the fabrication of chips in the industry came to maturity as the microelectronics industry shifted to "fabless" chip suppliers who exclusively sub-contract the production of externally manufactured semiconductors. Unlike IDMs, fabless chip suppliers own no fabrication capability and focus instead on the design, branding, and marketing of chips produced by merchant foundries. Currently, the top twenty fabless chip suppliers are based in the United States, Taiwan, and the European Union, according to 2010 data.[204]

[202] "More foundry competition means lower chip prices" (Digi-Key Corporation, 27 September 2011).
[203] Jeorge S. Hurtarte, Evert A. Wolsheimer, and Lisa M. Tafoya, *Understanding fabless IC technology* (Elsevier, Inc., 2007).
[204] "U.S.-based Companies Held 13 of the Top 20 Fabless Spots in 2010" (IC Insights Research Bulletin, 21 April 2011).

2010 Top 20 Fabless IC Suppliers

2010 Rank	2009 Rank	2008 Rank	Company	Headquarters	2008 ($M)	2009 ($M)	% Change	2010 ($M)	% Change
1	1	1	Qualcomm	U.S.	6,477	6,409	-1%	7,204	12%
2	3	2	Broadcom	U.S.	4,449	4,271	-4%	6,589	54%
3	2	—	AMD	U.S.	0	5,403	N/A	6,494	20%
4	6	4	Marvell	U.S.	3,055	2,690	-12%	3,592	34%
5	4	5	MediaTek	Taiwan	2,864	3,500	22%	3,590	3%
6	5	3	Nvidia	U.S.	3,660	3,151	-14%	3,575	13%
7	7	6	Xilinx	U.S.	1,906	1,699	-11%	2,311	36%
8	10	8	Altera	U.S.	1,367	1,196	-13%	1,954	63%
9	8	7	LSI Corp.	U.S.	1,795	1,422	-21%	1,616	14%
10	11	9	Avago	U.S.	905	858	-5%	1,187	38%
11	12	11	Novatek	Taiwan	829	819	-1%	1,149	40%
12	9	—	ST-Ericsson*	Europe	0	1,263	N/A	1,146	-9%
13	15	18	MStar	Taiwan	454	605	33%	1,067	76%
14	17	17	Atheros**	U.S.	472	543	15%	927	71%
15	16	12	CSR	Europe	695	601	-14%	801	33%
16	14	15	Realtek	Taiwan	534	615	15%	706	15%
17	13	10	Himax	Taiwan	833	693	-17%	643	-7%
18	18	16	PMC-Sierra	U.S.	525	496	-6%	635	28%
19	69	52	Trident	U.S.	149	85	-43%	558	556%
20	—	—	Lantiq	Europe	0	0	N/A	550	N/A
Top 20			—	—	30,969	36,319	17%	46,294	27%
Others			—	—	12,861	10,931	-15%	13,571	24%
TOTAL			—	—	43,830	47,250	8%	59,865	27%

*Represents the 50% share not accounted for by ST.
**To be purchased by Qualcomm in 2011.

Source: IC Insights' *Strategic Reviews Database*

Figure 5: Top 20 Fabless International IC Suppliers and Sales Volumes 2008—2010.
Source: IC Insights, *The McLean Report* (2011).

The pure IDM model has been weakening due to pressures to compete in an ever more populated field, and as the effects of the international economic downturn forced a record amount of wafer fabrication capacity to be taken off-line in 2009 and 2010 while companies attempted to consolidate and reduce costs by closing older fabrication facilities and adopting the fabless or fab-lite business model. The latter is a hybrid strategy in which a supplier maintains a portion of their fabrication capability, but subcontracts large volumes of routine production to merchant foundries.[205]

These diversified chip sourcing strategies, while promising to deliver greater profits and more rapid technology advancement, extends the upstream supply chain for end applications considerably, potentially exposing the end product to greater opportunities for exploitation by an adversary with enough sophistication to map the complete supply chain and identify points of vulnerability. According to industry analysts, as costs of foundry operations and internal manufacturing have continued to rise, even larger companies have begun shifting to fabless or fab-lite business models, especially in complex logic and microcomponents

[205] Hurtarte 8. Of the sixteen chip manufacturers contributing components to the common router examined for this study, at least one has gone fabless while at least two have embraced the fab-lite model.

integrated circuit markets.[206] Many integrated circuit suppliers who are not true IDMs maintain upstream relationships with merchant foundries.[207] Presently only four of the top fifteen companies by sales volume are located in the United States, complicating the task of tracing the sources of local inputs and design for components on a given IC.

At the chip foundry level, regardless of supply model, IC fabrication can be divided into a series of operations which are commonly grouped "front end of line" (FEOL) and "back end of line" (BEOL). FEOL processing refers to the formation of the transistors directly in the silicon wafer and culminates in the production of individual layers of etched silicon wafers which still require assembly into complete integrated circuits. The BEOL phase denotes the second portion of IC fabrication, during which the individual devices (transistors, capacitors, resistors, etc.) are interconnected with wiring on the wafer and those etched layers are bonded to result in a "chip" that will then proceed to testing, packaging and further testing operations. Each of these phases, FEOL, BEOL, packaging and testing can be, and often are, completed at different independently owned foundries. Even IDM and hybrid suppliers will distribute these operations, locating packaging and testing facilities (back end chip processing, not BEOL) physically close to their target market or where other economic benefit can be realized.

2010 Major IC Foundries

2010 Rank	2009 Rank	Company	Foundry Type	Location	2008 Sales ($M)	2009 Sales ($M)	09/08 Sales (%)	2010 Sales ($M)	10/09 Sales (%)
1	1	TSMC	Pure-Play	Taiwan	10,556	8,989	-15%	13,307	48%
2	2	UMC	Pure-Play	Taiwan	3,070	2,815	-8%	3,965	41%
3	4	GlobalFoundries	Pure-Play	U.S.	0	1,101	N/A	3,510	219%
4	5	SMIC	Pure-Play	China	1,353	1,070	-21%	1,555	45%
5	9	TowerJazz	Pure-Play	Europe	252	300	19%	510	70%
6	7	Vanguard	Pure-Play	Taiwan	511	382	-25%	508	33%
7	6	Dongbu	Pure-Play	South Korea	490	395	-19%	495	25%
8	8	IBM	IDM	U.S.	400	335	-16%	430	28%
9	12	MagnaChip	IDM	South Korea	346	262	-24%	420	60%
10	10	Samsung	IDM	South Korea	340	290	-15%	400	38%
11	11	SSMC	Pure-Play	Singapore	340	280	-18%	330	18%
12	15	X-Fab	Pure-Play	Europe	368	212	-42%	320	51%
13	14	Hua Hong NEC	Pure-Play	China	280	240	-14%	295	23%
14	13	TI	IDM	U.S.	315	250	-21%	285	14%
15	16	Grace	Pure-Play	China	230	180	-22%	260	44%
—	3	Chartered*	Pure-Play	U.S.	1,743	1,540	-12%	0	N/A

*Purchased by GlobalFoundries in 4Q09.

Source: IC Insights, company reports

Figure 6: 2010 major international IC foundries. *Source:* IC Insights, The McClean Report 2011.

[206] "TSMC First Pure-Play Foundry to Join Top-10 R&D Spenders" (IC Insights Research Bulletin, 13 January 2011).
[207] "Samsung lags in foundry rankings" (EE Times, 20 January 2011).

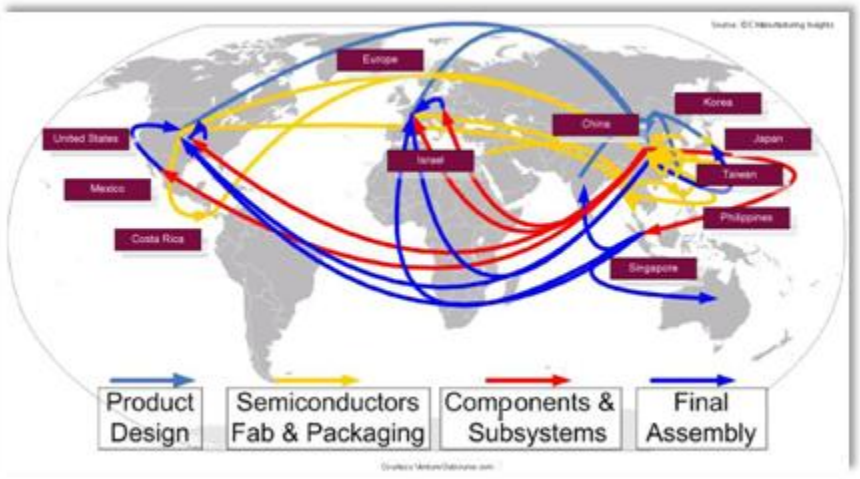

Figure 7: Example of global supply chain progression.

Source: Venture Outsource.[208]

Exploiting the Upstream IC Supply Chain

The complexity and versatility of the IC industry allows a single chip to incorporate circuits designed in locations around the globe by hundreds of people working at many firms. This global fragmentation of chip design and manufacture quickens the production pace and reduces the cost of new product development; but because the detection of rogue circuitry hidden among the hundreds of millions of transistors is difficult before the chip is shipped to its next location for integration onto a larger circuit, it also creates additional security and integrity risks.[209] A sophisticated adversary with access to highly skilled personnel and engineering resources could mount an upstream attack against manufacturers by modifying the software on programmable chips before they are shipped for integration into other products; the firmware to alter the data that it provides; or the internal circuitry of chips to create performance problems.[210] ***Without strict control of this complex upstream channel, a manufacturer of routers, switches or other telecommunications hardware is exposed to innumerable points of possible tampering, and must rely on rigorous and often expensive testing to ensure that the semiconductors being delivered are trustworthy and will perform only as specified, with no additional unauthorized capabilities hidden from view.***

Comprehensive testing of delivered semiconductor components can be costly, time prohibitive, and may negatively impact the life expectancy and reliability of the tested component. The detection rates for identifying intentionally altered products is often below

[208] Mark Zetter, "Economic drivers, challenges creating regional electronics industry" (Venture Outsource, December 2009).
[209] John Villasenor, "The Hacker in Your Hardware" (*Scientific American,* August 2010).
[210] McFadden.

the rate of unintentional manufacturing defects, which only adds to the challenges posed by the excessive cost and reliability of testing. Physical inspections and low cost testing techniques are suitable for addressing most counterfeit threats, but these physical inspections are often less effective against sophisticated forms of counterfeiting and generally unable to detect circuits containing malicious code, according to a recent study by the Institute for Defense Analysis.[211]

U.S. Government agencies have expressed interest in altering the means by which ICs and related hardware are manufactured, rather than attempting to fully secure existing production channels. Both the Defense Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Project Research Agency (IARPA) have issued requests for proposals to address different aspects of the problem, testing finished products and creating more trusted back end of line processing. IARPA's Trusted Integrated Chips (TIC) Program seeks proposals to develop split manufacturing processes whereby front end of line fabrication can be conducted offshore, leveraging the capacity and capabilities of the world's foundries while bringing BEOL operations into trusted U.S. facilities.[212] The goal of DARPA's Integrity and Reliability of Integrated Circuits (IRIS) program is to develop technologies to test the functionality of an integrated circuit and ascertain whether or not it has been tampered with, and to determine its useful lifespan.[213]

Increasingly, defense planners and industry analysts are concerned about the potential for an adversary to gain access to a component of the global telecommunications supply chain and insert corrupted elements such as chips or whole integrated circuits.[214] Deliberate modification of semiconductors upstream of final product assembly and delivery could provide an adversary with capabilities to gain covert access and monitoring of sensitive systems, to degrade a system's mission effectiveness, or to insert false information or instructions that could cause premature failure or complete remote control or destruction of the targeted system. The modifications need not be complex. One of the simplest modifications would be the degradation of the interconnects that distribute signals and provide power and ground to the various ICs, which will lead to premature failure under load. More complex attacks could introduce entirely new logic through the addition of extra transistors and circuitry.

In 2008, a group of researchers at the University of Illinois at Urbana Champaign designed and implemented a malicious CPU based on the LEON3 open source processor. This processor

[211] Sydney Pope, Brian S. Cohen, Vashisht Sharma, Ryan R. Wagner, Loren W. Linholm and Sherry Gillespie, "Verifying Trust For Defense Use Commercial Semiconductors." (Office of the Secretary of Defense, March 2010).
[212] IARPA, *Trusted Integrated Chips (TIC) Program Broad Agency Announcement, Solicitation Number: IARPA-BAA-11-09* (FedBizOps, viewed November 2011).
[213] *Integrity and Reliability of Integrated Circuits (IRIS), Solicitation Number: DARPA-BAA-10-33* (FedBizOps, viewed November 2011).
[214] See for example, *Defense Science Board Task Force on High Performance Microchip Supply;* Marianne Swanson, Nadya Bartol, and Rama Moorth, "Piloting Supply Chain Risk Management Practices For Federal Information Systems (NISTIR 7622)" (National Institute of Standards and Technology, June 2010).

demonstrated as a proof of concept the ability to design hardware that can support multiple types of attacks rather than designing a single specific software-based attack.[215] The Illinois researchers implemented three separate attacks: privilege escalation, password stealing and remote control of the operating system being run on the malicious processor. These actions required the addition of a small number of logic gates that were undetectable using nondestructive quality assurance testing methods. Current testing, reverse engineering, and fault-tolerance techniques are unsuitable for detecting digital side effects resulting from compromised ICs, making it difficult to identify deliberate modifications to a chip design by a rogue supplier.

Downstream Supply Chain Attacks

Targeting the downstream distribution channels supplying the intended victim organizations is a potentially less complex alternative to tackling the engineering and logistical complexities of penetrating the upstream semiconductor manufacturing supply chain itself. While numerous scenarios are possible, one that has proven most viable is the use of front companies operating as a reseller of specific branded equipment to U.S. distributors whose customers are priority targets for penetration. By providing counterfeit hardware containing Trojanized access built into the firmware or software loaded at the time of assembly, a foreign intelligence service or similar state sponsored entity could gain the accesses they seek.[216] Alternately, an adversary may attempt to inject finished counterfeit hardware into shipments of branded equipment destined for select U.S. resellers and distributors with high interest customers. Gathering the market intelligence on customer lists would not require extensive investment of time or collection resources by a professional foreign intelligence service. Armed with this information, multiple distributors could be potentially targeted in a single operation. Compromised hardware, designed to communicate covertly with the adversary operators once installed on the targeted network, would allow an adversary team to establish an access point from which to establish a more permanent presence. This approach is not without risk of discovery, particularly if the counterfeit goods are identified at any point in the shipping or installation process.

Unless the compromises to software or firmware are identified as espionage attempts to penetrate the supply chain, the incident would likely be prosecuted as one of dozens of counterfeiting cases uncovered annually by U.S. Customs and Border Patrol (CBP) agents. Both of these approaches would require the production of sophisticated counterfeits, more credible than those currently entering U.S. markets. The Federal Bureau of Investigation (FBI) has worked closely with CBP to identify fraudulent hardware, with some notable successes such as “Operation Network Raider” which has, as of May 2010, resulted in over 30

[215] Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou, "Designing and implementing malicious hardware" (USENIX LEET 2008). For more details on the Leon3 Processor, see Aeroflex Gaisler AB, "Leon3 Processor" (2008).

[216] Nation state adversaries are not the only source of threats in a downstream attack on the supply chain, but they are the most likely based on motive and resources necessary to engineer the compromise, and create and maintain the distribution channels to see the operation through to completion.

convictions and 700 seizures of counterfeit Cisco brand network hardware coming from China.[217]

China was the leading source country for counterfeit and pirated goods in 2011, representing 62% of all IPR seizures by domestic value, according to U.S. Department of Justice data.[218] Customs and Border Patrol agents reportedly made 541 seizures of Chinese sourced counterfeit computer and related hardware last year. While these numbers largely reflect criminal activity, the volume of counterfeit goods coming in precludes thorough testing of ICs for malicious compromises in these and other electronics parts, suggesting that even thwarted attempts at supply chain compromise for espionage purposes are unlikely to be identified easily.

According to the preliminary results from an ongoing Government Accountability Office (GAO) investigation initiated in late 2011 to identify the extent of availability for counterfeit military grade electronic parts on Internet purchasing platforms, all samples through a GAO established front company obtained have been identified as "suspect counterfeit." Though the study did not focus on any single country, all of the samples obtained originated from companies in China.[219]

While there is no direct evidence that activity such as the manufacture of counterfeit electronic components such as those purchased by GAO investigators is state sponsored, the operational impact of replacing hardware, and the resultant degraded performance of networks dependant on undiscovered counterfeits would be a significant resource drain, particularly if equipment failures occurred during operations or hostilities. Systems engineering and security best practices dictate removing all configuration settings from new hardware and manually enabling only those capabilities required. The appliance's operating system, however, is responsible for interpreting these configuration settings. Rootkit technology, while more commonly applied to servers and end-user systems, was shown to apply to the Cisco Internetworking Operating System (IOS)[220] in 2008.[221] In addition, pre-IOS code called the "bootstrap" is responsible for locating IOS and could be subverted via a supply chain inject to load alternate IOS code. In this way the rootkit version would then survive complete re-installation of IOS. To identify such an instrumentation of a router or switch would require costly and time-consuming forensic examination not described in the NSA SNAC Router Security Configuration Guide.[222]

[217] U.S. Department of Justice, "Departments of Justice and Homeland Security Announce 30 Convictions, More Than $143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware" (May 2010).
[218] Customs and Border Patrol Office of International Trade 30.
[219] GAO Testimony Before the Committee on Armed Services, "DOD SUPPLY CHAIN, Preliminary Observations Indicate That Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms" (U.S. Senate, 8 November 2011).
[220] Cisco IOS is the core operating system software on routers and switches worldwide, including U.S. federal government and military networks.
[221] "Rootkits on Cisco IOS Devices" (Cisco, 16 May 2008).
[222] U.S. National Security Agency, Report Number C4-040R-02, "Router Security Configuration Guide" (15 December 2005).

DOD has expressed awareness of these issues and has initiated a Supply Chain Risk Management (SCRM) policy and strategy to address these vulnerabilities. A pilot program is under way, with the objective of live application by FY 2016, to implement "a SCRM capability that integrates program protection planning, enterprise architecture, counterintelligence, information assurance, systems engineering, procurement, enhanced test and evaluation, and other measures to mitigate supply chain risk."[223] As was demonstrated by the GAO study, however, the level of scrutiny necessary to ensure component integrity, while striving to leverage the efficiency and economic benefit of the Internet and the broad availability of competing replacement products, may become prohibitively expensive and result in a significant choke point without greater international cooperation.

Corrupting the firmware and the supply chain for the U.S. Government or private sector companies could provide an adversary with deep penetration into these organizations; however, email borne attacks carrying malicious payloads or links to malicious sites are far less complicated and continue to enjoy high levels of success. Adversaries operating in the cyber domain against the United States are likely able to achieve many of their intelligence collection goals faster and cheaper by using these more traditional malicious software based attacks.[224]

Operational Challenges to Exploiting the Telecommunications Supply Chain

Despite the growing concern among policymakers and security professionals about supply chain vulnerability, an attacker seeking to implement a successful chip level compromise in the U.S. telecommunications supply chain actually faces a highly complex operational challenge. An adversary attempting to target a single U.S. government agency, network, or commercial entity by compromising upstream manufacturing must be able to predict where the compromised components will eventually be deployed or simply allow the compromised hardware to ship globally to all customers of a given manufacturer. The high degree of international fragmentation and vertical specialization in IC production described above means that an attacker may also have to map the complete chain of suppliers, to include identifying the point at which they could successfully implant a rogue design into the chip or IC during a specific production run, and then oversee the engineering design and manufacture of the compromise itself. The technical and operational complexity of such upstream penetrations may greatly limit the pool of candidates with the necessary resources to successfully mount such an effort.

- Successful implementation would likely require extensive technical R&D to verify that the proposed compromise would work as intended from an engineering perspective; this would require probable access to detailed designs of the specific chip or other

[223] U.S. Deputy Secretary of Defense, Report Number DTM 09-016, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems" (25 March 2010).
[224] Scott Borg, "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework" (The Internet Security Alliance, April 2009).

element of the IC being exploited, either through HUMINT recruitment, SIGINT collection, or through the cooperation of the manufacturer's executive leadership.

- The attacker must also determine if the objective is best served via a mass compromise of every IC being produced from a single foundry or sold by a specific integrator in the international market or whether to create a highly selective compromise that is only intended to affect a small number of end users and involve only a limited production run at the penetrated foundry. The latter course of action presents additional targeting and delivery challenges that must also be managed over the course of the operation.

- Many, though not all, of these operational questions presume cooperative access by the design or manufacturing firm whose product is going to be altered. Attempting these types of penetrations in a non-cooperative foundry environment only magnifies the complexity of the overall operation.

- If the target is a U.S. Government agency or military component, the attackers must ensure that their compromised product is successfully delivered into the approved procurement stream used by the targeted organization. Globally-based, just-in-time supply models coupled with the potential complexities of government procurement regulations only add to the variables against which an attacker must plan.

- A study on supply chain security by the Institute for Defense Analyses (IDA) noted that merely hiding the identification of end use customers of commercially available ICs may provide a degree of anonymity that could further inhibit a foreign adversary's ability to penetrate targeted networks with compromised firmware.[225]

The technical and logistical challenges associated with hardware supply chain compromises render these types of attacks generally feasible for only extremely well-resourced organizations, such as nation-state intelligence organizations that have the depth of expertise and access to necessary technical personnel to penetrate a supply chain with sophisticated firmware compromises. The level of sophistication likely involved in this type of operation could require years of painstaking preparation and work and not only physical access to production facilities but the ability to recruit insiders to influence the design or fabrication of a component. All of these steps must be done with sufficient operational security to avoid detection throughout the compliance measurement and testing phases of production, and then activate the Trojanized capabilities hidden in the component after delivery to the target organization.

Upon execution of the malware or use of the backdoor on the compromised component, the adversary running the operation must plan for the possible detection of their efforts yielding only a small window of access to a penetrated network. If the component compromise is

[225] Pope 75.

intended to alter the performance of a weapon system at a critical moment during a conflict, the need for access would be limited to a single instance when the uploaded malicious software is activated to achieve its desired effect—such as introducing some degree of error into the guidance system of a missile, unmanned aircraft or possibly a manned system during operation to cause malfunction or seeming operator error. This type of single-use access would likely be considered a "war reserve mode" by a foreign government and remain unused until the outbreak of actual hostilities, greatly reducing the possibility of detection by the victim.

A Comparative Analysis of Criminal vs. State-Sponsored Network Exploitation

Non-state criminal operators and state-sponsored professional intelligence or military actors typically operate in the same environment and sometime against similar classes of targets. This is an overlap that poses attribution challenges for information security professionals, policymakers, business leaders, and members of the law enforcement and intelligence communities, all of whom have uniquely different responses to these two categories of actors. Distinguishing between these categories of actors is not merely an academic or theoretical debate. The actions of each group, if left unchecked, have the potential to inflict serious damage to U.S. national security at multiple levels. Professional state sponsored intelligence collection not only targets a nation's sensitive national security and policymaking information, it increasingly is being used to collect intellectual property and trade secrets that have the potential to undermine the private sector's ability to compete and foster innovation.[226]

The easy availability of sophisticated anonymization tools have made attributing a given network penetration or data theft to a specific nation, group, or individual increasingly difficult for law enforcement and intelligence officials.[227] Similarly distinguishing a non-state criminal operation from a state-sponsored effort is difficult without a clear understanding of the types of data targeted. Some operational differences exist, however, between these categories of actors that if applied systematically to the analysis of intrusions and incident data will serve as a simple heuristic for classifying incidents.

Cyber Criminal Operational Profile: Non-state sponsored, online criminal activity is typically driven by one or more classes of motivation related to online social or political activism ("hacktivism"), amateurish attempts to gain notoriety or recognition ("script kiddies"), or financial gain, which is most typically associated with cybercrime.

Online social activism has the potential to cause significant harm to governments, organizations, and individuals depending on the methods and agenda of the attackers. Groups such as Lulzsec and Anonymous seeking to further a social agenda can reveal sensitive competitive information or embarrassing personal details about individuals targeted. Others such as the Wikileaks organization can do significant harm to national security by revealing sensitive intelligence operational details or diplomatic and policy discussions. In most cases the intent is not to cause harm. The zeal to affect change in an organization's or government's policy, however, can sometimes drive such groups to extremes, including attacking websites of foreign governments or those supporting them. One prime example is the case of the "hacker war" that occurred between pro-PRC and pro-U.S. activists following the EP-3 incident in 2000 and CNN's comments on the Beijing Olympics that many felt were

[226] "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2010-2011" (Office of the National Counterintelligence Executive, October 2011): 3.
[227] D. Wheeler and G. Larsen, "Planning For the Future of Cyber Attack Attribution" (House of Representatives Subcommittee on Technology and Innovation, Committee on Science and Technology, 15 July 2010).

derogatory.[228] Social activism and prank attack groups such as Lulz Security, Anonymous and others gain relevance in ways similar to terrorist organizations – through public or target recognition of their exploits and positive identification of the responsible organization or social cause to which they profess allegiance.

The so-called "script kiddie" amateurs are generally inexperienced attackers seeking peer status or exercising criminal curiosity, and though they usually are not a significant threat to well-prepared organizations, they can do considerable harm to those who are unprepared. More mature professional criminal organizations that are well resourced and comprised of often highly skilled members have established vast money making empires where incidents can sometimes cause tens of millions of dollars in damages.

The online opportunities for a talented and criminally minded entrepreneur are continually growing as more sensitive financial and personal data moves through servers and networks around the world daily. Income can also be generated from authoring criminal software ("crimeware"), or from using crimeware to establish and maintain botnets for hire, spam distribution, theft of banking credentials and other liquid or fungible types of data. In April, 2011, a criminal case was brought against the operators of the "Coreflood" botnet, which involved over 2.3 million computers engaged to commit fraud against an unknown number of victims.[229] In 2010, IBM's threat intelligence unit documented more than 8,000 new vulnerabilities, a 27 percent rise from 2009 while public exploit releases were also up 21 percent from 2009 to 2010.[230]

Criminal data theft operations typically do not place value on compromising and maintaining access to specific servers or end-user machines, but seek instead high degrees of flexibility and agility, often in environments with enormous variety and targeting options. In criminal operations where attackers may remain on a given system for only minutes before moving to the next, little value is placed on preserving access to any specific system nor is care exercised to ensure their actions aren't being monitored—except when their toolkit provides stealth or tenacious anti-tampering measures as a built-in feature,[231] choosing to rely on the their agility as a defense against detection or arrest. Botnet management schemes, such as dynamic "fast-flux" DNS in which the attacker uses a domain name service (DNS) technique common in many botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies, create a rapidly moving target for law enforcement.[232] The operator is given the freedom to continue their work without needing to linger and risk detection. When an asset of particular

[228] David G. Wiencek, "South China Sea Flashpoint" (The Jamestown Foundation, 24 July 2001); Jose Nazario, "Politically Motivated Denial of Service Attacks" (Arbor Networks, July 2009); Dancho Danchev, "Chinese Hacktivists Waging People's Information Warfare Against CNN" (22 April 2008).
[229] U.S. Federal Bureau of Investigation, "United States District Court—District of Connecticut - No. 3:11 CV 561(VLB)" (11 April 2011).
[230] IBM, "Visualizations: Vulnerabilities Per Year" (30 March 2011).
[231] jackk, "Reversing the source of the ZeroAccess crimeware rootkit" (*Offensive Computing*, November 2010).
[232] See for example M. Knysz and Xin H., "Charlatans' Web: Analysis and Application of Global IP Usage Patterns of Fast-Flux Botnets" (University of Michigan, 2009).

value is discovered, the fluid infrastructure provides the attacker a transport network that is only trusted long enough to steal that targeted data. If a specific compromised host has technical difficulty or presents a risk to the operator's anonymity, shifting away to another requires little effort and presents minimal impact to the operation.

State sponsored intelligence operations tend to work in exactly the opposite way. Rather than having the flexibility to make rapid shifts from one target to the next to avoid detection, these operators often have a more limited number of targets to choose from, particularly if they have been tasked to collect engineering data related to a specific weapons system or a policy position to be presented in an upcoming diplomatic summit; information such as this is often stored at a specific location within a single network. Criminals, in contrast, rarely have to collect a specific credit card number or the personally-identifiable information of selected individuals. State sponsored intelligence operators tasked to collect against a specific set of requirements, must in effect, look for specific sets of data often within large networks run by professional information security staffs.

State-Sponsored Operational Profile: A review of the scale, focus, and complexity of the many network exploitation campaigns attributed to state-sponsored groups reveals a degree of financial, staffing, and analytic resources that exceed what even the largest organized cybercriminal operations could likely manage for even short periods of time. ***The goals of these groups are generally to support espionage operations, to conduct reconnaissance and instrument military networks with sensors or "sleeper" tools for later use during a conflict, to steal commercial competitive data or intellectual property, or in more limited cases, to demonstrate capabilities to deter a rival state. Recently, a new class of operation has emerged: the exploitation of networks to gain information that can be used to enable these other operations***.

- Activities attributed to state sponsored operators often appear to target data that is not easily monetized in underground criminal online auctions or markets.

- Highly technical defense engineering information, operational military data, or government policy analysis documents rarely if ever appear to be a priority for cybercriminal groups, suggesting that analytic models that account for the likely identity of the end user of the stolen information as well as identify the affiliation and identity of the group or individual at the keyboard may have more efficacy and predictive power for counterintelligence purposes than those that do not.

Many of the government, defense and other commercial companies targeted by long term network exploitation have large, multilayered information security operations run by experienced professionals. Yet their adversaries continue to penetrate these defenses and maintain a presence long enough to gather valuable intelligence on their defenses, map their networks, and obtain the means to create access that allows them to log into these organizations as legitimate users. While a handful of criminal organizations may have

sufficient resources to maintain an operation against a single target for months, the vast majority of them do not, nor does the financial incentive exist for them to try.

A brief survey of discussion threads in a popular members-only online hacking forum, Hackforums.net, suggest that there is little to no interest in the kinds of technical and policy data typically targeted in incidents attributed to state-sponsored groups. The forum contains over 1.4 million discussion threads comprised of over 14 million individual messages among 220,000 users. Keyword searches for relevant terms yielded no hits for any engineering data, business competitive information, or victims of publicly disclosed penetrations. The topics of discussion include attempts at monetizing stolen information, distribution of attack software, tutorials, gaming, exploitation of various hardware and software systems, covert communication, anonymization, support, communication and recruitment. The discussions regarding items for sale included:

- Credit cards
- Card verification values (CVV2)
- Online payment system accounts
- Compromised social network accounts
- Botnet access
- Attack services for hire
- Money laundering
- Offshore banking

While the findings are preliminary and limited to a single, albeit extremely large hacker website, the complete absence of any reference to the availability of high tech data or business development plans for any organization among 14 million unique posts at this site suggests that the online criminal underground is not targeting the defense, policy, or business operations data as a practice. Exceptions may exist and plausible scenarios may exist in which freelance hackers are hired by state entities to perform network exploitation on a contract basis. As a matter of definition, however, such activities can reasonably be considered "state-sponsored" given that the work is done for a single government customer and the stolen data is not being offered for sale to the highest bidder in underground hacker markets as is typical for stolen financial data or personally identifiable information. These findings are preliminary; a broader more in-depth study of multiple hacker sites and discussion boards—particularly closed, invitation only environments—and websites was beyond the scope of the present study, but could provide more precise indication of the consistency of this separation of targeted data types between criminal and state sponsored operations. This information may aid counterintelligence analysts and information security professionals in more reliably identifying attacker origin in future incidents and to understand the types of data that may be at risk.

Attack Sophistication as a Predictor of State Sponsorship: The operational sophistication of the publicly disclosed incidents attributed to state actors, such as China, does not uniformly

suggest that the operators used advanced tools or tradecraft for the initial compromise, privilege escalation, lateral movement and data exfiltration. ***A review of industry reporting on incidents such as Google's Aurora penetration, the operations associated with the 2009 GhostNet incident or the 2011 "Shady Rat" activities indicates that the groups employed only what was minimally necessary to succeed against the targeted networks, suggesting that they were often as advanced as their target environment demanded.*** [233] Typically, the groups active in these incidents use relatively common or unsophisticated techniques to gain initial access to their targeted networks. Once the breach is attained, however, their behavior suggests prior detailed reconnaissance as they display more sophisticated knowledge of the network environments they were targeting.

- Initial penetration of Google was via a chat message containing an innocuous-looking link to a photo sharing website. The malware served up at that site attacked a previously undisclosed vulnerability on the victim's web browser providing the attackers the ability to establish communications with the compromised computer and move laterally deeper into Google's network. The success of this operation pivoted on reconnaissance which fueled effective social engineering; the attackers' ability to craft a credible link for the pre-selected victim Google employees to click on.

- The activities of the groups profiled in the 2009 GhostNet operations suggest that they assembled highly detailed logical maps of the networks they penetrated, likely done over long periods of time when they operated undetected.

In some incidents the attacks are portrayed in media and industry reports as "advanced" only because the targeted organization was unable to stop them or detect the operators once they have successfully established a presence in the victim's network. The problem arises when many victim organizations simply don't have the resources to maintain large or highly skilled information security organizations with the depth to adequately defend against these types of adversaries.

- In the widely publicized "Operation Shady Rat" incident the victims were simply emailed links to websites that downloaded the malware embedded in a common office-format document allowing the attackers to establish a communications channel to compromised machine and assume control. This type of targeted email attack has been common for over ten years and is a standard method for attempting to establish a presence within a targeted network.

- In the Aurora attacks against Google, the operators exploited a previously unknown vulnerability (often referred to as a "zero day" exploit) in Internet Explorer 6, an older version of the popular web browser software, which downloaded remote administration malware and compromised the machine. The operators then established an encrypted communications channel through which they assumed

[233] HBGary, <http://www.hbgary.com/press/hbgary-threat-report-operation-aurora>.

control of the targeted machine. This control allowed them to move laterally within Google's—or any other organization's—unprotected internal network, according to publicly available forensic analysis of the event.[234] These techniques had been observed frequently in network intrusions, both criminal and state sponsored, over the previous decade and were not new or unique to Google.

The publicly disclosed evidence linking Chinese state sponsorship to the Google intrusion is compelling but still largely circumstantial. No hard evidence links China to either of these campaigns, and the type of information stolen in both incidents noted above is not easily monetized in online criminal underground markets where stolen credit card numbers are sold, money is laundered, or malware is offered for sale. Information on political dissidents, corporate intellectual property and business operations has little appeal among this demographic.

- Analysis of the malware by third party specialists identified only a small component of the overall code that clearly had a Chinese pedigree; the information targeted was both Google source code and email accounts reportedly of Chinese human rights activists, suggesting a political as well as economic motivation. The IP addresses for the C2 nodes discovered during the forensic investigation were attributed to a Chinese college that has been linked in the past to alleged state sponsored network exploitation activity.[235]

- While none of these data points in isolation offers conclusive proof of Chinese state sponsorship, the reconnaissance techniques and apparent targeting priorities are indicative of other intrusions attributed to Chinese operators.[236]

Analysis of forensic data associated with penetrations attributed to sophisticated state sponsored operators suggests that in some operations multiple individuals are possibly involved, responsible for specific tasks such as gaining and establishing network access, surveying portions of the targeted network to identify information of value, and organizing the data exfiltration. One role is an entry or "breach team" tasked only with gaining entry and maintaining a flexible, redundant presence in the target network (essentially "picking the lock" and ensuring not only that the door stays open, but that there are multiple doors available if the one being used is "closed"). Once the breach team has successfully established access to the network, a possible second team or individual conducts the data reconnaissance and ultimately locates and exfiltrates targeted data.

---

[234] HD Moore, "Reproducing the Aurora IE Exploit" (15 January 2010); Ryan Paul. "Researchers Identify Command Servers Behind Google Attack" (*Ars Technica*, January 2010).

[235] Joe Stewart, ''Operation Aurora: Clues in the Code,'' *Secureworks*, January 19, 2010. http://www.secureworks.com/research/blog/research/20913/

[236] Bryan Krekel, George Bakos, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrop Grumman Corp, prepared for the US-China Economic and Security Review Commission, October 9, 2009, p. 61. http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

- Compartmentation may drive this dynamic to use different individuals or groups: the first team or operator does not need to know the details of what is being targeted by the second team or operator, or because of the specialized skills required for each phase of an intrusion. These explanations are, however, largely speculative as the fidelity of data on these incidents almost never provides insight into the internal communications, identity, or relationship dynamics of the actual people behind these intrusions.[237]

- This type of task oriented structure requires multiple skill sets, possibly requiring several individuals to complete one operation. This model, if accurate, also implies some means of recruiting, organizing, and managing a team like this and ensuring proper completion of a given mission. If this model is indeed accurate and it is being replicated across dozens of intrusions over time, then that oversight structure must be proportionately larger and more complex as well.

- Once the breach team or individual has secured a foothold on the first victim's computer, they also continue to collect information about this machine's security configuration, settings, and related system information to solidify their presence, sometimes by sniffing and stealing passwords from authentication systems, collecting user email to support future deceptive attacks, gather network usernames, group membership information and directory listings of network shared folders.

These attackers have also demonstrated an awareness of a targeted organization's information security measures according to forensic analysis of attacker activity, and appear able to alter their operations to avoid detection, reflecting the highly detailed reconnaissance that they—or others on their behalf—conduct. They likely use tools or techniques that are only as sophisticated as they need to be for the environment in which they are operating, holding their more capable tools in reserve until genuinely required.

- Attackers have demonstrated some ability to respond to adjustments in security configurations to ensure maximum time "on station" to accomplish their collection mission. These responses include, but are not limited to, shifting to stealthier communications channels, jumping to different C2 servers, the rapid deletion of toolkits upon detection of defender presence and the harvesting of configuration files to support further target analysis.

- The individuals responsible for maintaining access have demonstrated flexibility in responding to unexpected changes in network defenses by the targeted organization, suggesting they prepare for these contingencies in advance, similar to conducting an

[237] "Establishment and management of an organization so that information about the personnel, internal organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties." Don Philpott, ed., *A Guide to Federal Terms and Acronyms* (2011).

"enemy course of action" analysis. Generally, this preparation has involved the pre-placement of redundant communication channels, C2 nodes on multiple external servers, and multiple breach points in a targeted network (usually other computers in the targeted network that have already been compromised and are held in reserve until needed).

- The malware that these operators employ generally tries to communicate with (or "beacon" to) a pre-established command and control server located in a variety of countries. This beaconing can continue for extended periods of time before the operators are ready to engage, establish a connection with and then take control over the victim system.

Additional individuals or teams probably tasked with the collection of the actual targeted information have demonstrated greater skill and highly detailed knowledge of the targeted networks. Their efforts to locate and move data off of the network often involves techniques that place a premium on redundancy, stealth and comprehensiveness of preparation and attention to detail.

- Using network intelligence likely gathered during earlier reconnaissance efforts, these collection teams have in some cases copied the data from the servers and workstations to a second server that acts as a "staging point" where they compress, encrypt, segment and replicate it before distributing it through encrypted channels out of the targeted organization to multiple external servers that act as "drop points." These drop points may also play an obfuscation role, complicating investigative efforts to identify the data's final destination.

Driving Up Attacker Resource Costs: Attacker techniques typically shift significantly or increase in sophistication when their target's defenses improve, consuming additional attacker resources for tool and malware development. Shifts in defender techniques may also force an attacker to invest additional funds for more experienced personnel to maintain existing levels of activity against their targets.

- The March 2011 penetration of security firm RSA was likely the result of this dynamic. Two state sponsored groups successfully breached the company's networks and exfiltrated significant amounts of data related to the encryption algorithm of the company's authentication token system widely deployed in government and industry.[238]

- The theft of the authentication algorithms was an intermediate step to provide the attackers the necessary tools to breach the security systems of defense contractors

[238] Steve Ragan, "RSA's 'Trial by Fire' Caused by Two State-Sponsored Groups" (*Security Week,* 12 October 2011).

and others who relied on RSA products to safeguard remote access into their corporate networks.[239]

- In effect, the attackers' strategy for targeting RSA was analogous to robbing the locksmith for a master key rather than picking individual locks.

The RSA penetration was a well planned, multistage operation that began with reconnaissance of remote authentication methods, followed by profiling of RSA employees to craft credible emails and ended with the breach of at least one U.S. defense contractor, Lockheed Martin.[240]

- Lockheed Martin is the prime contractor for the F-35 and F-22, both 5th generation fighters that will form the core of all U.S. air combat requirements in coming decades. The majority of the technology or programs developed at the company would likely have little "street value" among the online criminal underground.

- Lockheed Martin's sophisticated information security environment may have motivated these groups to seek other, game changing tactics that would provide them with the access they required to meet their operational tasking and intelligence collection requirements.

- Had the company's perimeter remained porous, additional complexity would not have been warranted. It is revealing to note that while the attackers had the requisite depth of penetration to collect significant criminally marketable data, there is no evidence that there was attempted or successful theft of anything other than the necessary elements to conduct follow-on espionage operations, according to a review of media reporting of the incident.[241]

[239] Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed Martin" (*New York Times*, 4 June 2011): B1.
[240] Ibid.
[241] Christopher Drew and John Markoff, "Data Breach at Security Firm Linked to Attack on Lockheed Martin."

Collaboration of U.S. and Chinese Information Security Firms: Risks and Reality

Collaboration between U.S. and Chinese information security firms, while not common to date, has raised concerns over the potential for illicit access to sensitive network vulnerability data at a time when the volume of reporting about Chinese computer network exploitation activities directed against U.S. commercial and government entities remains steady.

To date, the joint venture between Huawei Shenzhen Technology Company, Ltd. and Symantec, Inc. is the only major partnering of a large U.S. information security firm with a Chinese high technology entity. The partnership prompted widespread media coverage and public discussion; however, little substantive information has ever surfaced to link this relationship, forged in 2007, to the increased exploitation of any U.S. network or to documented Chinese penetration of IT supply chains used by the U.S. Government. This suggests that joint ventures or similar strategic partnerships between U.S. and Chinese firms in the information security industry may not, as a category, pose an inherently greater risk to U.S. network security or overall U.S. national security.

In November 2011, the partnership announced that after four years of operations, Huawei would buy out Symantec's portion, giving Huawei full ownership of the company.[242] Analysts have asserted that from a market standpoint, the joint venture has been a success: Symantec had achieved its goals of Chinese market and hardware appliance market penetration, as well as a strong return on its initial investment in the joint venture; and Huawei had gained access to Symantec's storage and security solutions for integration into Huawei's cloud computing and appliance initiatives. Through the full acquisition of Huawei Symantec, Huawei will launch directly into server, storage, and IP networking markets, including U.S. markets.[243] Symantec has also announced that it will continue to use Huawei as a hardware supplier for its North American customers.[244]

At present no other information security firms have publicly announced plans for similar deals in China. The absence of such relationships does not prevent future attempts by Chinese information security firms to pursue strategic partnerships with U.S. companies, particularly if the Chinese entities believe that such relationships provide expanded access to U.S. or other Western markets. Chinese companies attempting to partner with a U.S. information security firm will likely be forced to address significant consumer skepticism or bias as a result of ongoing media coverage of alleged Chinese state sponsored hacking activity against government and commercial networks.

[242] Huawei Symantec, "Huawei Acquires Symantec Stake in Huawei Symantec Joint Venture" (14 November 2011).
[243] Joseph Kovar, "Symantec To Sell Stake In Huawei Symantec Joint Venture To Huawei" (*CRN*, 15 November 2011).
[244] Larry Walsh, "Symantec Will Continue to Partner with Huawei" (Channelnomics, 17 November 2011).

- Following the formation of the Huawei-Symantec joint venture in 2007, industry analysts and policymakers raised concerns over potential security vulnerabilities from the perceived Huawei access to Symantec technologies, and the presumed strengthening of PRC civil and military information security capabilities.

- Anti-virus vendor McAfee has maintained a presence in China since 2009 when it established reseller partnerships with both Neusoft and CS&S (China National Software and Services) who have become premier partners for McAfee products in China. McAfee's arrangement, however, does not include a joint venture and appears to be a sales and distribution relationship.

- Potential Chinese entrants into the U.S. or any international market will also face scrutiny of products and services from the broader information security and software industries. Any future collaborations would need to be capable of being certified and evaluated by international industry standards.

- Kingsoft, one of China's largest software and antivirus vendors is a member of Microsoft Virus Information Alliance, a vendor group comprised of 16 top tier information security vendors in the international market.[245] Kingsoft's collaboration in this forum enables provides access to the latest threat data on new malicious software and attack vectors observed by other alliance members, however, Kingsoft has not attempted to leverage its presence in the group to form more formal business relationships with American peer companies.

The risks arising from future partnerships between U.S. or other Western information security firms and Chinese IT firms are primarily related to the loss of intellectual property and erosion of long term competitiveness, the same threats faced by many U.S. companies entering partnerships in China. Intellectual property theft is a concern for virtually all U.S. businesses operating in China, according to a 2011 survey conducted by the US-China Business Council.[246] That U.S. information security firms entering partnerships to operate in domestic Chinese markets would likely face the same pressures to share IP and risk having IP stolen via insiders or network exploitation or both, is a continuing problem in many sectors and regions, according to this same US-China Business Council Study.

- The 2011 US-China Business Council report on IPR enforcement in China noted that despite gradual improvement in some regions of China and in select industries, "patent, trademark, copyright, and trade-secret infringement remains a major concern for U.S. companies operating in China."[247]

[245] Kingsoft North America, "Kingsoft Joins Microsoft Virus Information Alliance Becoming the First Chinese Member" (22 June 2009).
[246] US-China Business Council. "2011 Special 301 Review." 15 February 2011.
[247] Ibid 1.

- Consumer or retail oriented anti-virus products would not likely contain highly sensitive data with the potential to significantly improve China's military IW capabilities. Firms with expertise, however, in the management of information security for extremely large enterprises with sophisticated detection suites have more potential to aid PRC government network defense capabilities.

- The strategic value of the U.S. firm's technology would likely determine how directly the PRC government or military would attempt to involve itself. Currently, the only data point for an assessment of this is the Huawei-Symantec partnership; thus, analytic conclusions about how and what benefits potentially accrue to the state, military, or commercial sectors are difficult to make.

- The Chinese Government has had a longstanding practice to require foreign firms in strategically important industries to either transfer key components of intellectual property or invest significant amounts to establish R&D centers in China staffed by Chinese employees. Many companies claim this results in the eventual loss of critical IP and often the dissolution of the partnership to allow the Chinese entity to operate as a competitor using the foreign firm's IP.[248]

Following the formation of the Huawei-Symantec joint venture, industry critics noted the potential sensitive signature data to pass to the Chinese authorities, whom many believe are behind the extensive exploitation of U.S. commercial and government networks. The concern arises from the possibility that sensitive customer reporting and signature data could enable the Chinese CNE operators to understand which of the operations or tools were working and which were not. In reality, most information of this type is either publicly available or available via subscription and would not require elaborate and expensive mergers and acquisition process to acquire.

- Partnering with an American or other Western anti-virus vendor, for example, does not necessarily allow the Chinese partner to obtain signature data earlier than legitimate participation in industry consortia such as the Microsoft Virus Information Alliance. Thus a merger-and-acquisition approach by a Chinese IT firm to gain access to sensitive information security customer data does not present any real temporal advantage and would not likely be a motivation to enter into a long term partnership.[249]

- Of likely greater benefit to the Chinese side, however, would be the access to the strategically important technology, tools, and business practices of the U.S. company

[248] Dan Harris, "An ABC To Losing Your China IP" (China Law Blog, 22 October 2011); see also Lou Kilzer, "Apple tries to avoid Motorola's mistakes in China" (*Pittsburgh Tribune-Review*, 3 April, 2011).

[249] The Microsoft VIA is an international partnership created by the Microsoft Corporation in association with various antivirus software vendors. Alliance members exchange technical information about newly discovered malicious software (malware) so they can quickly communicate information to customers. See http://en.wikipedia.org/wiki/Virus_Information_Alliance.

that would allow the Chinese sector to improve across the industry or within priority areas of government or military network management.

A formal partnership may also provide the Chinese entity the opportunity to gain market share or access via the U.S. partner's supply or distribution chain. Huawei-Symantec Ltd. last year formed two strategic partnerships with U.S. companies that again created controversy for the perceived threat of Huawei access to U.S. government and commercial networks, this time indirectly through reseller relationships established with U.S. distributors and IT service companies.[250]

- Huawei-Symantec successfully used this reseller channel sales conduit to secure its first high performance storage cluster contract with the University of Tennessee's National Center for Computational Engineering, a supercomputer facility that does computational modeling, simulation, and design for a variety of applications and customers, including U.S. Department of Defense. A Huawei-Symantec channel partner, MPAK Technology based in San Diego, was responsible for the sale.[251]

- Using a reseller relationship potentially allows Huawei-Symantec to avoid previous U.S. Government blocks on their products and potentially funnel products into U.S. government or commercial IT infrastructures, according to information security industry analysts, raising additional concerns over Huawei's ability to access or supply U.S. government networks or hardware.[252] The underlying concern by many in the information security and defense communities is that Huawei, while being publicly blocked by U.S. lawmakers from selling directly to the U.S. Government, is quietly securing access to U.S. Defense Department and intelligence community customers through collaborative partnerships that to date have not been contested.

To the extent that potential future collaborations between U.S. information security firms and Chinese counterparts are largely R&D in nature, there may be greater potential for IP theft that could materially advance Chinese network defense capabilities in state organizations. There is a potential motivation for exploiting network trust relationships to gain access to targeted IP. The foreign partner, if influenced by its government, may be motivated to exploit network trust relationships to gain access to targeted IP belonging to its U.S. partner. This risk is not limited to Chinese business partners or to the security industry: it is present in numerous industries, sectors, and countries in which the U.S. business may operate.

[250] Chris Mellor, "Huawei-Symantec takes big step with Force10" (*Channel Register,* 1 March 2011).
[251] Eli Lake, "Computer Lab's Chinese-Made Parts Raise Spy Concerns" (*The Washington Times,* 16 August 2011); See also University of Tennessee Chattanooga, "UTC SimCenter: National Center for Computational Engineering."
[252] Jeffrey Carr, "China's Silent Cyber Takeover?" *The Diplomat,* April 17, 2011

Conclusion:

The People's Liberation Army today is entering its second decade of a sustained modernization drive that has generated remarkable transformation within the force. The Revolution in Military Affairs (RMA), the transformational concept that has radically altered Western approaches to modern warfare, has put information technology and the ability to control the flow of data at the core of how modern militaries organize, equip, and fight. The PLA is pursuing the means to seize and occupy the "information high ground" in the modern battlespace by employing these concepts and new technologies to exert control over information and information systems.

While the modernization of China's military hardware continues to capture headlines, the rapid development of a comprehensive C4ISR infrastructure, linking platforms, personnel, and operations, is arguably the most transformative of all PLA efforts currently underway. Unifying disparate information systems and enabling coordination between geographically dispersed units has the potential to generate greater lethality without the need to radically overhaul the existing force structure. Doctrinally, this process of networking its force structure is referred to as Fighting Local Wars Under Conditions of Informationization. Success in this environment means attaining near total situational awareness of the battlespace while limiting an adversary's ability to do the same.

Computer network operations (attack, defense, and exploitation) have become fundamental to the PLA's strategic campaign goals for seizing information dominance early and using it to enable and support other PLA operations throughout a conflict. During peacetime, computer network exploitation has likely become a cornerstone of PLA and civilian intelligence collection operations supporting national military and civilian strategic goals.

The apparent expansion of China's computer network exploitation (CNE) activities to support espionage has opened rich veins of previously inaccessible information that can be mined both in support of national security concerns and, more significantly, for national economic development. Information that previously required close-in human intelligence (HUMINT) access, necessitating the long-term development and recruitment of individuals with access to targeted information, is now easily obtained by sending a phishing email to the unsuspecting targets.

Military operations have similarly benefitted from the unlimited range and precision of network based weapons and intelligence collection opportunities. Holding an adversary's logistics and communications capabilities at risk previously required kinetic options (accurate missiles, quiet submarines, special operations forces, or advanced maritime strike aircraft) to physically target key communications nodes. PLA leaders understand now that tactical level employment of CNA tools used with sufficient precision can achieve dramatic strategic outcomes with the potential to alter a campaign. Conversely, as the PLA deploys more sophisticated information systems and grows increasingly reliant upon them for successful

military operations, it also must also protect itself from the same network vulnerabilities as its high-tech adversaries. This imperative places computer network defense (CND) on an equal footing with its counterparts in the CNO triad.

While CNO is appealing to China's military leaders as a tool for offense and intelligence collection, its ease of use and development do not fully explain China's apparent eagerness to employ CNO to further national strategy. CNO tools used in the support of military contingencies like a Taiwan or South China Sea crisis also carry appeal for their ability to reach strategic targets in the United States and Western Pacific without requiring the use of conventional weapons and kinetic strikes. Ballistic missiles, airstrikes and troop landings have attribution "fingerprints" like none other, whereas CNO actions often have none. Furthermore, the use of kinetic options is a clear *casus belli* under international law and leaves less ambiguity about a likely U.S. response. The skillful application of CNA or CNE tools, by contrast, can exploit the vagaries of international law and policy surrounding nation state responses to apparent network attack to delay or degrade a potential U.S. military response to a crisis.

The PLA is augmenting its developing CNO capabilities by relying on inputs from China's commercial IT industry, academia, and civilian and military research institutions. The private sector is funding R&D with state grants, as well as its own resources in some cases, in areas that have relevance to improving information security and offensive tools. A defined group of military and civilian universities have emerged as centers of excellence or hosts of state laboratories devoted to CNO research. The PLA's extensive network of research institutes is also making breakthroughs in many aspects of information security and computer science. The 2010 development at a PLA university of what was then the world's fastest supercomputer demonstrated the high quality and focus of current research. It also underscores the inherently dual-use qualities of information technology that allow the PLA to leverage the "spin-on" effect of new innovation from China's commercial IT sector.

Telecommunications hardware notables such as Huawei, Zhongxing (ZTE), and Datang maintain relationships with the PRC government to varying degrees, ranging from commercial contracting, to supporting research institutes, and funding R&D for dedicated military or dual-use technologies. Such relationships continue to fuel speculation in the United States and other Western nations about potential network attack or exploitation vectors created by the growing presence of these and other Chinese IT companies in global telecommunications infrastructure markets.

These concerns are magnified by the globally diffuse telecommunications supply chain that appears to allow multiple points of access to an adversary intent on corrupting hardware components, such as integrated circuits or larger components they support. The complexity of the global high-tech supply chain, however, may carry inherent defensive advantages. Obfuscating the end user of a chipset during the design and manufacturing processes has the potential to act as a deterrent by making the problem more logistically complex for most adversaries. Other measures that can diminish the chances that a compromised chipset

successfully reaches its intended target could also dramatically decrease the perceived return on investment in upstream supply chain compromises. Downstream supply chain penetrations of hardware resellers and distributors, however, continue to pose significant law enforcement and counterintelligence challenges to the United States.

Taken in the aggregate, recent developments in Chinese CNO applications and R&D point to a nation fully engaged in leveraging all available resources to create a diverse, technically advanced ability to operate in cyberspace as another means of meeting military and civilian goals for national development. Computer network operations have assumed a strategic significance for the Chinese leadership that moves beyond solely military applications and is being broadly applied to assist with long term strategy for China's national development.

Appendix A: Universities Using Major Grant Programs for IW Research

Organization Name	Acronym	Chinese Name	URL	State Secrecy Academy	242	s219	115	863	973
Southeast University	SEU	东南大学	www.seu.edu.cn		x	x	x	x	x
Harbin Institute of Technology	HIT	哈尔滨工业大学	www.hit.edu.cn	x	x	x	x	x	x
Zhejiang University	ZJU	浙江大学	www.zju.edu.cn		x	x	x	x	
Beijing University of Posts and Telecommunications	BUPT	北京邮电大学	www.bupt.edu.cn		x		x	x	x
Beijing Jiaotong University	BJTU	北京交通大学	www.njtu.edu.cn		x		x	x	x
Anhui University	AHU	安徽大学	www.ahu.edu.cn		x		x	x	x
Dalian University of Technology	DLUT	大连理工大学	www.dlut.edu.cn		x		x	x	x
Shanghai Jiaotong University	SJTU	上海交通大学	www.sjtu.edu.cn		x	x		x	x
Harbin Engineering University	HRBEU	哈尔滨工程大学	www.hrbeu.edu.cn		x	x		x	x
University of Shanghai for Science and Technology	USST	上海理工大学	www.usst.edu.cn		x	x		x	x
Beijing Institute of Technology	BIT	北京理工大学	www.bit.edu.cn		x			x	x
Xi'an University of Electronic Science and Technology	XUEST	西安电子科技大学	www.xidian.edu.cn		x			x	x
Peking University	PKU	北京大学	www.pku.edu.cn		x			x	x
University of Electronic Science and Technology of China	UESTC	电子科技大学	www.uestc.edu.cn		x			x	x
Xi'an Jiaotong University	XJTU	西安交通大学	www.xjtu.edu.cn		x			x	x
Beijing University of Technology	BJUT	北京工业大学	www.bjut.edu.cn		x			x	x
Northwestern Polytechnical University	NWPU	西北工业大学	www.nwpu.edu.cn	x	x			x	x
CERNET CERT (hosted at Tsinghua University)	CNCERT	中国教育和可就计算机网紧急响应组	www.ccert.edu.cn		x			x	x
Henan Polytechnic University	HPU	河南理工大学	www.hpu.edu.cn		x			x	x
Tsinghua University	THU	清华大学	www.tsinghua.edu.cn		x			x	x
Huazhong University of Science and Technology	HUST	华中科技大学	www.hust.edu.cn		x			x	x
Northwest A&F University	NWSUAF	西北农林科技大学	www.nwsuaf.edu.cn		x			x	x
Wuhan University of Science and Technology	WUST	武汉科技大学	www.wust.edu.cn		x			x	x
Nanjing University of Technology	NJUT	南京工业大学	www.njut.edu.cn		x			x	x
Sichuan University	SCU	四川大学	www.scu.edu.cn		x			x	x

Organization Name	Acronym	Chinese Name	URL	State Secrecy Academy	242	s219	115	863	973
Xi'an University of Posts and Telecommunications	XUPT	西安邮电大学	www.xupt.edu.cn		x			x	x
University of Science and Technology of China	USTC	中国科学技术大学	www.ustc.edu.cn		x			x	x
Soochow University	SUDA	苏州大学	www.suda.edu.cn		x			x	x
Shandong University	SDU	山东大学	www.sdu.edu.cn		x			x	x
Guangxi University of Technology	GXUT	广西工大院	www.gxut.edu.cn		x			x	x
Wuhan University	WHU	武汉大学	www.whu.edu.cn				x	x	x
Changchun University of Science and Technology	CUST	长春理工大学	www.cust.edu.cn				x	x	x
Nanjing University of Information Science and Technology	NUIST	南京信息工程大学	www.nuist.edu.cn				x	x	x
Hunan University	HNU	湖南大学	www.hnu.edu.cn				x	x	x
Sun Yat-Sen University	SYSU	中山大学	www.sysu.edu.cn	x			x	x	x
Ningbo University	NBU	宁波大学	www.nbu.edu.cn				x	x	x
Shanghai Finance University	SHFC	上海金融大学	www.shfc.edu.cn				x	x	x
Nanyang Normal University	NYNU	南阳师范学院	www.nynu.edu.cn				x	x	x
Tongji University	TJU	同济大学	www.tongji.edu.cn			x		x	x
Shanghai Dianji University	SDJU	上海电机大学	www.sdju.edu.cn			x		x	x
Fudan University	FDU	复旦大学	www.fudan.edu.cn			x		x	x
Nanjing University	NJU	南京大学	www.nju.edu.cn	x		x		x	x
Shaoxing University	SXU	绍兴文理学院	www.usx.edu.cn					x	x
National University of Defense Technology	NUDT	国防科学技术大学	www.nudt.edu.cn					x	x
PLA Information Engineering University	PLAIEU	解放军信息工程大学	www.plaieu.cn					x	x
Nanjing University of Science and Technology	NJUST	南京科学技术大学	www.njust.edu.cn					x	x

Appendix B: Chinese Grant Programs Supporting Information Security Research

Chinese Name	English Name
全国信息安全标准化技术委员会	National Technical Committee for Information Security Standardization
公安部第三研究所	Third Research Institute of the Ministry of Public Security
北京电子科技学院开放基金资助项目	Beijing University of Electronic Science and Technology Open Foundation
华为基金项目	Huawei Foundation Project
国家“九七三”重点基础研究发展规划项目基金	National 973 Basic Research Program
国家“八六三”高技术研究发展计划项目基金	National 863 High Technology Research and Development Program Foundation
国家115科技研究基金	Ministry of State Security 11 Project
国家242信息安全计划	National 242 Information Security Program
国家S219信息安全应用示范工程	S219 National Information Security Demonstration Project
国家信息安全保障计划	National Information Security Guarantee Program
国家发改委信息安全产业化项目	National Development and Reform Committee of the Information Security Industrialization Program
国家大学生创新性试验计划	National Innovation Research Program for University Students (NSRIT)
国家密码理论发展基金	National Code Theory Development Foundation
国家科技集成计划	National Key Technology R&D Program
国家自然科学基金资助项目	National Natural Sciences Foundation
国家计委产业化示范工程	National Planning Commission on Industrialization Demonstration Projects

国家计委信息安全产业化项目	National Planning Commission on Information Security Industrialization Projects
国家软科学研究计划	National Soft Science Research Program (MOST and National Advisory Committee for State Informatization)
国家高技术研究发展计划	National Information Security Support Program
新世纪优秀人才支持计划	New Century Excellent Talent Support Program
江苏省保密局项目	Jiangsu Province Administration for the Protection of State Secrets Program
江苏省自然科学基金	Jiangsu Province Natural Sciences Foundation
电子政务信息系统安全体系结构研究	E-Government Information System Security Architecture Study
省市重点科技攻关计划项目	Province and City-level Key Science and Technology Problem Solving Programs
上海市重点科学建设项目基金	City of Shanghai Key Scientific Project Foundation
上海市科学技术委员会基金	City of Shanghai Science and Technology Committee Foundation
上海市科技攻关项目	Shanghai City Scientific and Technological Project
江苏省重点实验室基金	Jiangsu Province Key Laboratory Foundation
常州市高技术研究重点实验室项目	Changzhou City High Technology Key Laboratory Project
河南省重点科技攻关项目	Henan Province Key Scientific and Technological Project
上海市自然科学基金	Shanghai City Natural Sciences Foundation

Glossary of Technical Terms

Backdoor – A method of regaining remote control of a victim's computer by reconfiguring installed legitimate software or the installation of a specialized program designed to allow access under attacker-defined conditions. Trojan horse programs and rootkits often contain backdoor components.

Basic Input/Output System (BIOS) A preinstalled program used during startup on IBM PC compatible computers. The CPU initially executes instructions in the BIOS, after which a bootloader program is executed which loads the computer's operating system.

Brute force – A class of attack whereby multiple attempts are made to compromise a system by cycling through different combinations of attack until one is successful. Repeated password-guessing is an example of brute-force. This type of attack is highly likely to be detected during and after execution by CND monitoring systems.

C2 – Command and control. In the context of computer network operations, a communications method or a component thereof to maintain remote control of an operational asset such as a compromised computer.

Central Processing Unit (CPU) – The integrated circuit responsible for executing instructions, performing calculations and other data manipulations in a computer.

Cloud computing A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.(See http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)

Complementary Metal Oxide Semiconductor (CMOS) – A type of semiconductor commonly used in battery-powered memory on personal computers to store the date, time, and system startup parameters.

Coder – A computer programmer or one who writes computer programming language code.

Compromise (verb) – To gain unauthorized access to a computing system.

Computer Network Attack (CNA) – Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (See: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf).

Computer network defense (CND) – Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within information systems and computer networks (See: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf).

Computer network exploitation (CNE) – Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks (See: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf).

Computer network operations (CNO) Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations (See http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf).

Denial of Service Attack (DoS) – A class of computer network attack designed to deny an adversary access to computing resources, data or networks. Common attacks include: flooding to consume available network bandwidth, exploitation of protocols to consume available memory or CPU capacity, settings modification and physical destruction. Common variants include DDoS (Distributed DoS) and DRDoS (Distributed-Reflected DoS).

Digital Certificate (or simply Certificate) A computer-generated record that ties the user's identification with the user's public key in a trusted bond. The trust is based on registration/identification policy enforced by a third party, Certification Authority. The certificate contains the following: identification of the Certification Authority issuing the certification; the user; the user's public key; and is digitally signed by the issuing Certification Authority. (See http://jitc.fhu.disa.mil/pki/terms_and_definitions.html)

Distributed denial of service (DDoS) – A class of attacks that results in the exhaustion of computing or communications resources by engaging many intermediate computers to simultaneously attack one victim. These intermediate attack systems are often previously compromised and under the control of the attacker.

Electronic Countermeasure (ECM) – That division of Electronic Warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, through the use of electromagnetic energy. There are three sub-divisions of ECM: Electronic Jamming, Electronic Deception and Electronic Neutralization. (See http://jcs.dtic.mil/j6/cceb/acps/acp167/ACP167J.pdf)

Electronic Warfare (EW) – Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.

Hacker – An individual who uses computer technology in ways not originally intended by the vendor. Commonly the term is applied to people who attack others using computers. For the purposes of this discussion, hackers are subdivided as follows:

- • **Script kiddies**: Unskilled attackers who do not have the ability to discover new vulnerabilities or write exploit code, and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages.

- • **Worm and virus writers**: Attackers who write the propagation code used in the worms and viruses but not typically the exploit code used to penetrate the systems infected. Their goal is notoriety. Their sub-goals are to cause disruption of networks and attached computer systems.
- • **Security researchers and white hat operators**: This group has two subcategories: bug hunters and exploit coders. Their goal is profit. Their sub-goals are to improve security and achieve recognition with an exploit.
- • **Professional hacker-black hat**: Individuals who get paid to write exploits or actually penetrate networks; this group also falls into the same two subcategories as above. Their goal is also profit (See: http://www.uscert. gov/control_systems/csthreats.html).

Hacktivism – Computer hacking intended to communicate a social or political message, or to support the position of a political or ideological group. Hactivism activities include data theft, website defacement, denial of service, redirects and others.

Hacktivist – An attacker who practices hacktivism.

Information Warfare (IW) – Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks (See: http://www.jpeocbd.osd.mil/packs/DocHandler.ashx?DocId=3712)

Intrusion Detection System (IDS) – A computer or network monitoring system that matches observations against patterns of known or suspected unauthorized activity.

Motherboard – Primary printed circuit board used in computer systems. Major components such as CPU, DRAM, BIOS and peripheral controllers are either soldered directly in place or plugged into sockets on the motherboard.

NIPRNET – Non-secure Internet Protocol Router Network. The unclassified network of the U.S. Department of Defense providing Internet access as well as interconnectivity to DoD users and facilities.

Phishing – The practice of enticing a victim to visit a website or other online resource with the intention of stealing credentials, financial information such as bank accounts, or credit card numbers. Phishing attacks generally involve an email claiming to come from a trusted entity such as a bank or ecommerce vendor, with a link to a website and the instructions to click the link and take actions once at the website.

Random Access Memory (RAM) – The volatile working memory on a computing device, used to temporarily store data and program code. Dynamic RAM (DRAM) and Static RAM (SRAM) are two main variants, both being volatile memory; the contents of which are lost when the system is powered off.

Read Only Memory (ROM) – Hardware used for storage of long-term static data. BIOS is one use for semiconductor ROM, as is flash EEPROM (Electrically erasable programmable ROM). Optical examples include CD-ROM and DVD-ROM.

Rootkit A piece of software that can be installed and hidden on the victim computer without the user's knowledge. It may be included in a larger software package or installed by an attacker who has been able to take advantage of vulnerability on the victim machine. Rootkits are not necessarily malicious, but they may hide malicious activities. Attackers may be able to access information, monitor user actions, modify programs, or perform other functions on the targeted computer without being detected (See: http://www.uscert.gov/cas/tips/ST06-001.html).

Side channel attack – An attack on a cryptographic system whereby data from other dependent systems is measured from which inferences can be made. Power consumption, timing analysis and acoustic emanations are example data sources for side-channel attacks. (See http://www.scientificamerican.com/article.cfm?id=hackers-can-steal-from-reflections)

Spearphishing – A targeted phishing attack against a select group of victims, usually belonging to a single company, school, industry, etc. "Spearphishing" is commonly used to refer to any targeted email attack, not limited to phishing.

Strings – sequences of one or more data values that represent printable characters.

Trojan horse An apparently useful program containing hidden functions that can exploit the privileges of the user (running the program), with a resulting security threat. A Trojan horse does things that the program user did not intend. Trojan horses rely on users to install them, or they can be installed by intruders who have gained unauthorized access by other means. Then, an intruder attempting to subvert a system using a Trojan horse relies on other users running the Trojan horse to be successful (See: www.cert.org/advisories/CA-1999-02.html).

PACOM – United States Pacific Command is one of six Unified Combatant Commands of the United States Armed Forces with an area of responsibility encompassing all territory from the US West Coast to the western border of India, and from Antarctica to the North Pole. The command presently has approximately 325,000 US service personnel.

TRANSCOM United States Transportation Command provides intermodal transportation across the spectrum of military operations. TRANSCOM is comprised of three component commands: the Air Force's Air Mobility Command, the Navy's Military Sealift Command, and the Army's Military Surface Deployment and Distribution Command.

Virtual Private Network (VPN) – Extension of a physical network to remote locations across the Internet, using cryptographic protections on all communications.

Zero day exploit – An attack against a software vulnerability that has not yet been addressed by the software maintainers. These attacks are difficult to defend against as they are often undisclosed by the vendor until a fix is available, leaving victims unaware of the exposure.

Bibliography

"75770 Unit Holds Training Assemblies On New Training Program." *Zhanshi Bao*, 11 December 2008. OSC ID CPP20090130563001.

"78006 Unit Conducts Information Security Check in Office Facilities." *Zhanqi Bao*, 13 November 2009.

Aeroflex Gaisler AB. "Leon3 Processor." 2008. <http://www.gaisler.com/cms/index.php?option=com_content&task=view&id=13&Itemid=53>.

"Agilent Technologies and Datang Telecom Group Establish Joint Research Lab to Accelerate Development of Next-Generation Wireless Technology in China." BusinessWire (13 October 2011). <http://www.businesswire.com/news/home/20111013005985/en/TRADE-NEWS-Agilent-Technologies-Datang-Telecom-Group>.

"Apparent Text of PRC Medium- and Long-Term S&T Program Guidelines for 2006-2020." Xinhua Domestic Service, 9 February 2006. OSC ID CPP20060209005001.

Beijing Jiaotong University. "*2009 Niandu Shuangyu Jiaoxue Shefan Kecheng jianshe Xiangmu Shenbao Biao—Shujuku Xitong Ruanjian Gongcheng*" (2009 Bilingual Education Demonstration Course Development Project Report—Database System Software Project). 26 May 2009. <http://wenku.baidu.com/view/e9f27fdb6f1aff00bed51ee5.html>.

Beijing University of Posts and Telecommunications. "*Beijing Youdian Daxue*" (Beijing University of Posts and Telecommunications). <www.bupt.edu.cn>. Viewed November 2011.

"*Beijing Youdian Daxue Xiaochang Fang Binxing Jianjie*" (Profile of Beijing University of Posts and Telecommunications Professor Fang Binxing). Renmin Wang. <http://edu.people.com.cn/BIG5/145827/154647/9284460.html>. Viewed November 2011.

Blasko, Dennis. "PLA Ground Force Modernization and Mission Diversification: Underway in all Military Regions." in Roy Kamphausen, Andrew Scobell, eds. *Right Sizing the People's Liberation Army: Exploring the Contours of China's Military.* U.S. Army Strategic Studies Institute, September 2007.

Borg, Scott. "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework." The Internet Security Alliance, April 2009. <http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf>."

Budui 5 Yue Renshi Biandong Huizong" (Summary of Personnel Changes May 2009). 14 June 2009. <http://www.360doc.com/content/09/0618/15/145380/_3944145.shtml>.

Cao Shuanze. "*Jituan Jun Jidong Fangwei Zuozhan Xinxi Zhan De Jizhong Zhanfa*" (Information Warfare Tactics in Group Army Mobile Defensive Operations). *Junshi Xueshu* (Military Art Journal) (1 December 2003). OSC ID CPP20080313623001.

Cao Yan et al. "Fuzzy Evaluation Model for Effectiveness of Network Attack Based on Generalized Operators." *Jisuanji Yingyong Yanjiu*, 1 August 2009. OSC ID CPP20101008670003.

Cao Zhangrong, Wu Runbo, and Luo Dong, eds. *Xinxihua Lianhe Zuozhan* (Informationized Joint Operations). PLA Publishing House, 2008.

Cao Zhi. "Hu Jintao Emphasizes Importance of Reform and Innovation in Promoting Development of Military Training." Xinhua Asia-Pacific Service, 27 June 2006.

Chen Dingrong and Dai Yu. "Setting Off a New Upsurge in Training With Preparation for Military Struggle in Mind." *Guangzhou Zhanshi Bao*, 30 September 2005. OSC ID CPP20051220318009.

Chen, Jeff and Andrei Chang. "Organization and Combat Capability of PLA Ground Forces." *Kanwa Asian Defense Review* 35 (September 2007).

Chen Shanzhi. "Datang Telecom Technology & Industry Group." July 2009. <http://www.nmi.org.uk/assets/files/China-Inward-Mission/Datang.pdf>.

Cheng, Dean. *PLA Views of Space: The Prerequisite for Information Dominance,* Center for Naval Analyses, October 2007

"Chengdu Military Region (MR) 78006 Unit Excels In Informatization Building." *Chengdu Zhanqi Bao*, 24 September 2008.

"Chinese Military Exercises in 2010 Highlight Five Characteristics." *PLA Daily*, 21 January 2011. OSC ID CPP20110122702002.

Chinesecivilization2. "*[CCTV-7 Junshi Keji 2011-07-16] Wangluo Fengbao Lai Le / Wangluo Zhanzheng 2/2*" ([CCTV-7 Military Science and Technology 2011-07-16] The Network Storm Is Here / Network War 2/2). Youtube, 27 July 2011. <http://www.youtube.com/watch?v=L_Wu1HIZbBk>.

"*Chongqing Shi Wanzhou Qu Di San Jie Ren Da Daibiao—Jiang Jian*" (Third People's Congress Chongqing Wanzhou District Representative—Jiang Jian). Baidu. <http://baike.baidu.com/view/1285087.htm>. Viewed November 2011.

Cliff, Roger, et al., *Entering the Dragon's Lair: Chinese Anti-Access Strategies and Their Implications for the U.S.,* RAND Corp, 2007

Customs and Border Patrol Office of International Trade. *Publication # 0153-0112, Intellectual Property Rights Fiscal Year 2011 Seizure Statistics 2011.* U.S. Customs and Border Protection, 2012. <http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/pubs/seizure/ipr_seizures_fy2011.ctt/ipr_seizure_fy2011.pdf>.

Dai Qingmin. "Innovating and Developing Views on Information Operations." *China Military Science* (4-2000). OSC ID CPP20000911000150.

Dai Qingmin. "On Integrating Network Warfare and Electronic Warfare" (*Tan Wanglun Yi Tiao Zhan*). *China Military Science* (1), 2002. OSC ID CPP20020624000214.

Danchev, Dancho. "Chinese Hacktivists Waging People's Information Warfare Against CNN." 22 April 2008. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>.

Datang Telecom. "*Datang Dianxin Keji Chanye Jituan*" (Datang Telecom Technology & Industry Group). <http://www.datanggroup.cn/templates/T_Contents/index.aspx?nodeid=98>. Viewed November 2011.

Datang Telecom. "Datang Telecom Technology Co., Ltd." <http://www.datang.com/en/index.asp>. Viewed November 2011.

Datang Telecom. "*Dianxin Kexue Jishu Di Yi Yanjiu Suo*" (First Research Institute of Telecommunications Technology). <http://www.fritt1957.com/index.asp>. Viewed November 2011.

Datang Telecom. "Tenth Institute of Electronics." <http://www.datanggroup.cn/yjsb/websnew/zhuye/dzshs.htm>. Viewed November 2011.

"Datang Telecom Technology Co Ltd (600198.SS) Company Profile." Reuters. <http://www.reuters.com/finance/stocks/companyProfile?symbol=600198.SS>. Viewed November 2011.

"Datang Telecom Technology Co., Ltd." Bizearch.com. <http://www.bizearch.com/company/Datang_Telecom_Technology_Co_Ltd_357810.htm>. Viewed November 2011.

Defense Science Board Task Force on High Performance Microchip Supply. Office of the Under-Secretary of Defense for Acquisition, Technology, and Logistics, February 2005.

Ding Guodong. "*Mianxiang Luntan He Xinwen De (redacted) Jiance*" ((redacted) Monitoring of Forums and News). Chinese Academy of Sciences. <www.ict.cas.cn>.

Ding Liang et al. "Research on Covert Techniques of Kernel-Mode Rootkits Under Windows." *Jisuanji Gongcheng Yu Sheji* (Computer Engineering and Design), October 2006. <www.cnki.net>.

diviner, "*Tongxin Rensheng–Huawei Jishu Youxian Gongsi Dongshi Zhang Sun Yafang Jieshao*" (Communications Lifestyle–Introduction to Huawei Technology Co., Ltd. Chairwoman Sun Yafang). *Tongxin Ren Jia Yuan (Communications Home)*. China Communications Network (March 9, 2005). <bbs.c114.net/archiver/?tid-51066.html>.

Drew, Christopher and John Markoff, "Data Breach at Security Firm Linked to Attack on Lockheed Martin." *New York Times*, 27 May 2011. <www.nytimes.com/2011/05/28/business/28hack.html>.

Drew, Christopher. "Stolen Data Is Tracked to Hacking at Lockheed Martin." *New York Times*, 4 June 2011.

Duan Yajun, Wu Chang, and Li Chengen. "Analysis of Anti-Jamming Performance of JTIDS System." *Zhuangbei Zhihui Jishu Xueyuan Xuebao* (Journal of the Academy of Equipment Command and Technology) 18.5 (October 2007).

East Fortune. "Telecommunications Science and Technology Institute About _ tenth Datang Telecom." <http://guba.eastmoney.com/look,600198,1009170152.html>. Viewed November 2011.

Easton, Ian and Mark Stokes. "China's Electronic Intelligence (ELINT) Satellite Development." Project 2049 Institute, 23 February 2011. <http://project2049.net/documents/china_electronic_intelligence_elint_satellite_developments_easton_stokes.pdf>.

Fan Yunyu. "Great Firewall Father Speaks Out." *Global Times Online*, 18 February 2011. OSC ID CPP20110218722003.

FedBizOps. *Integrity and Reliability of Integrated Circuits (IRIS), Solicitation Number: DARPA-BAA-10-33.* <https://www.fbo.gov/index?id=30191c1ba1db9c257723e48b97d4c155>. Viewed November 2011.

Fifth Research Institute. "*Wu Suo Jieshao*" (About the Fifth Institute). <http://5ritt.datanggroup.cn/about.asp>. Viewed November 2011.

Finkelstein, David. "China's National Military Strategy: An Overview Of The "Military Strategic Guidelines." In Roy Kamphausen and Andrew Scobell, eds. *Right Sizing The People's Liberation Army: Exploring The Contours Of China's Militar*y. U.S. Army Strategic Studies Institute, September 2007.

Finkelstein, David. "The General Staff Department of the Chinese People's Liberation Army: Organization, Roles, & Missions." in James Mulvenon and Andrew N. D. Yang, eds. *The People's Liberation Army as Organization Reference Volume v1.0.* RAND Corp., 2002.

"Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2010-2011," Office of the National Counterintelligence Executive, October 2011. <http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf>.

Fourth Research Institute. "*Yewu Jieshao*" (Description of Products). <http://www.telfri.net/about.asp>. Viewed November 2011.

Fourth Research Institute. "*Dianxin Kexue Jishu Di Si Yanjiu Suo*" (Fourth Research Institute of Telecommunications Technology). <http://www.telfri.net/>. Viewed November 2011.

Fourth Research Institute. "*Kuandai Wuxian Yidong Duomeiti Tongxin Xitong*" (M4000 Broadband Wireless Mobile Multimedia Communication System). <http://www.telfri.net/ShowNews.asp?ID=989>. Viewed November 2011.

GAO Testimony Before the Committee on Armed Services. "DOD SUPPLY CHAIN, Preliminary Observations Indicate That Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms." U.S. Senate, 8 November 2011. <http://www.gao.gov/assets/590/586136.pdf>.

"Guangzhou Military Region Article on System-Based Combined Arms Training." *Zhanshi Bao*, 25 February 2011. OSC ID CPP20110504503001.

Guo Qingbao and Zhuang Juanjuan. "Major steps in accelerating informationization in the South Korean military." *National Defense and Armed Forces Building in the New Century and New Age.* Military Yiwen Press, 2008.

Han Xinwen, Gao Junguang, and Yang Baoqing. "Application Study of Information Countermeasures 'Blue Force' in Base Training." *Junshi Yunchou Yu Xitong Gongcheng* (Military Operations Research and Systems Engineering) 24 2 (June 2010).

Harbin Institute of Technology. "Full List of Professors." <http://newcs.hit.edu.cn/base_teacher/F>. Viewed November 2011.

Harbin Institute of Technology. "*Benke Sheng Zhaosheng*" (Undergraduate Admissions). <www.cs.hit.edu.cn/?q=node/31>. Viewed November 2011.

Harbin Institute of Technology. "*Xinxi Duikang Jishu Yanjiu Shi*" (Information Conflict Technology Laboratory). <http://www.cs.hit.edu.cn/?q=node/207>. Viewed November 2011.

Harris, Dan. "An ABC To Losing Your China IP." China Law Blog, 22 October 2011. <http://www.chinalawblog.com/2011/10/an_abc_to_losing_your_china_ip.html>.

Hartnett, Dan. *Towards a Globally Focused Chinese Military: The Historic Missions of the Chinese Armed Forces.* Center for Naval Analyses, June 2008. OSC ID CPP20080606325001.

HD Moore. "Reproducing the Aurora IE Exploit." 15 January 2010. <http://www.blog.metasploit.com/2010/01/reproducing-aurora-ie-exploit.html>.

Herrick, Joel. "CCTV documentary reveals hacking tool, links Chinese government to cyber attacks." Shanghaiist, 24 August 2011. <http://shanghaiist.com/2011/08/24/new_evidence_links_chinese_governme.php>.

"Highlights -- PRC Military Forums in August 2011." Open Source Center, 1 September 2011. OSC ID CPP20110902090001.

Hu Junhua and Liu Feng'an. "Approved by Chairman Hu and the Central Military Commission: The General Staff Department Promulgates the 'General Plan for Military Training Reform During the '12th Five-Year Program' Period'." *PLA Daily*, September 23, 2011.

Huawei Symantec. "Huawei Acquires Symantec Stake in Huawei Symantec Joint Venture." 14 November 2011. <www.symantec.com>.

"Huawei Annual Report Details Directors, Supervisory Board for First Time." Open Source Center, 5 October 2011. OSC ID FEA20111005022749.

Hurtarte, Jeorge S., Evert A. Wolsheimer, and Lisa M. Tafoya. *Understanding fabless IC technology.* Elsevier, Inc., 2007.

IARPA. *Trusted Integrated Chips (TIC) Program Broad Agency Announcement, Solicitation Number: IARPA-BAA-11-09*. <https://www.fbo.gov/index?id=36a5148742778693073399edc40f321>. Viewed November 2011.

IBM. "Visualizations: Vulnerabilities Per Year." 30 March 2011. <http://www-958.ibm.com/software/data/cognos/manyeyes/visualizations/vulerabilities-per-year>.

Included in Plan." *Zhanqi Bao*, 8 June 2011. OSC ID CPP20110903478001.

"Information Engineering University." China Military Online, March 2008. <http://english.chinamil.com.cn/site2/special-reports/2008-03/04/content_114849.htm>.

Information Office of the State Council of the People's Republic of China. "China's National Defense in 2006." 29 December 2006. <http://english.chinamil.com.cn/site2/news-channels/2006-12/29/content_691844.htm>.

Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Docket No. R-1128). Federal Reserve System, 7 April 2003.

Interference Technology. "2009 Microwave Industry Exhibition Invitation." 17 February 2009. <http://www.interferencetechnology.cn/act/388464.asp>.

"Iron Fist-2009 Exercise: Red Versus Blue Confrontation of Systems." CCTV-13, Beijing. 23 November 2009. Television. OSC ID CPP20091123017001.

jackk. Reversing the source of the ZeroAccess crimeware rootkit. *Offensive Computing*. <http://www.offensivecomputing.net/?q=node/1669>. Viewed November 2011.

Jamshidi, Mo. "System-of-Systems Engineering—a Definition," IEEE SMC 2005, 10-12 October 2005. <http://ieeesmc2005.unm.edu/SoSE_Defn.htm>.

Janczewski, Lech J. and Andrew M. Colarik, eds. *Cyber Warfare and Cyber Terrorism*. IGI Global, 2008.

Javvin Technologies. *Network Dictionary*. Javvin Technologies, 2007.

Jiang Rui and Song Yubo. "Dongnan Daxue Kewai Yanxue Jiangzuo" (Southeast University Extracurricular Research Lecture Series). <http://wenku.baidu.com/view/e9f27fdb6f1aff00bed51ee5.html>. Viewed November 2011.

Jiang Xueyou. "Enhancing Functional Awareness, Strengthening Direction of Work - Mobilization Department Director of Military Region Headquarters Department Ling Feng

Talks About National Reserve Forces Building." *Chengdu Zhanqi Bao*, 29 December 2005. OSD ID CPP20060221318006.

Jin Bo, Zhang Bin, and Wang Zhi-hai. "Analysis and Standardization of Intranet Security Technology." *Information Security and Communications Privacy*, July 2007.

Jin Guanghu, Gao Xunzhang, Li Xiang, and Chen Yongguang. "ISAR Image Cross Scaling Method for Ballistic Targets Based on Image Registration." *Xitong Gongcheng Yu Dianzi Jishu* (Journal of Systems Engineering and Electronics) 32 12 (1 December 2010).

Job592.com. "Yang." <http//www.job592.com/cv/081004/person60007.html>. Viewed November 2011.

"*Junyong Anquan jishu Fangfan Chanpin Di Si Pi Yi Renzheng Chenggong*" (Fourth Installment of Military Security Products Certified). 25 January 2010. <http://info.secu.hc360.com/2010/01/251148228300.shtml>.

Kamphausen, Roy, David Lai, and Andrew Scobell, eds. *The PLA at Home and Abroad: Assessing the Operational Capabilities of China's Military*. U.S. Army Strategic Studies Institute, June 2010.

Kilzer, Lou. "Apple tries to avoid Motorola's mistakes in China," *Pittsburgh Tribune-Review* (Pittsburgh, PA), 3 April, 2011. <http://www.pittsburghlive.com/x/pittsburghtrib/news/nation-world/s_730463.html#ixzz1bm9G7jpo>.

King, Samuel T., Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou. "Designing and implementing malicious hardware." USENIX LEET 2008. <http://www.usenix.org/event/leet08/tech/full_papers/king/king.pdf>.

Kingsoft North America. "Kingsoft Joins Microsoft Virus Information Alliance Becoming the First Chinese Member." 22 June 2009. <http://kingsoftna.com/news/joins-ms-virus-info-alliance/>.

Knysz, M. and H. Xin. "Charlatans' Web: Analysis and Application of Global IP Usage Patterns of Fast-Flux Botnets." University of Michigan, 2009. <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA535046>.

Korneev, Victor and Andrew Kiselev. *Modern Microprocessors, Third Edition*. Cengage Charles River Media, 2004.

Kovar, Joseph. "Symantec To Sell Stake In Huawei Symantec Joint Venture To Huawei." *CRN* (15 November 2011). <www.crn.com>.

Lake, Eli. "Computer Lab's Chinese-Made Parts Raise Spy Concerns." *The Washington Times,* 16 August 2011. <http://p.washingtontimes.com/news/2011/aug/16/computer-labs-parts-raise-spy-concerns>.

"Lanzhou MR 1st Technical Reconnaissance Bureau Visits Qilihe." Qilihe People's Government Affairs, 20 January 2009. <http://www.qlhzwdt.com/qlhweb/news_view.asp?newsid=3369>.

Li Jinzhong. "Energetically Expand and Deepen Preparations for Military Struggles" (*Dali tazhan he shenhua junshi douzheng zhunbei*). *PLA Daily*, 7 January 2010.

Li Li and Liu Zongfeng. "New-Type Militia Detachments 'Draw Swords' on Ground, at Sea, in Air and in Space." *Nanjing Renmin Qianxian* (Nanjing People's Frontline), 28 September 2009. OSC ID CPP20100222090008.

Li Li. "A preliminary exploration of models and patterns for informationization in foreign militaries." *National Defense and Armed Forces Building in the New Century and New Age*. Military Yiwen Press, 2008.

Li Suiping. "Network Warfare Technology and Its Development Trend." *Nanjing Dianzi Gongcheng Shi* (Nanjing Electronics Engineer) 01 68 (March 2007).

Li Yan and Wang Jinfa. *Junmin Ronghe Da Zhanlue* (Military-Civilian Fusion Grand Strategy). National Defense University Press, October 2009.

Li Yanbin, Zhang Ce, and Wu Hongqi. "Information Systems Based System of Systems Operations Command Capability and Study of Its Application." China Military Science 5 (2010).

Li Yun. "*Jiefangjun Zongcanmoubu Tongxinbu Gaibian Wei Zongcanmoubu Xinxihuabu*" (PLA General Staff Department Communications Department Reorganized Into the Department of Informationization). Xinhua, 30 June 2011. <http://mil.news.sina.com.cn/2011-07-01/0436654762.html>.

Liu Feng'an. "Chinese Military Exercises in 2010 -- Comprehensively Increasing Core Military Capability." *Junshi Shijie Huakan* (1 December 2010). OSC ID CPP20110310503003.

Liu Lifeng. " *Liqing Tixi Zuozhan De Jiben Neihan*" (Clarify Basic Connotations of 'System of Systems' Operations). *PLA Daily*, 27 January 2011.

Liu Zhongbao. "Data Mining: An Important Technique for Seizing Information Superiority" *National Defense and Armed Forces Building in the New and Century New Age*. Military Yiwen Press, 2008.

Luo Ji, Zhang Kejin. "Creating Own 'Blue Army' for the Opposing Force." *Zhanshi Bao*, 10 March 2008.

"Made in China processors power world's fastest supercomputer." *Want China Times*, 25 March 2011. <www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1204&mainCatID=12&id=20110325000025>.

"Majestic and Powerful Forces, Fierce and Sweeping Actions Over a Thousand Miles—Review of, and Thoughts About, the 'Mission Action-2010C' Trans-region Mobile Exercise." *Zhanqi Bao*, 10 November 2010. OSC ID CPP20101222478002.

"Manpower Mobilization Capability Should Be Improved by Strengthening Three Areas." *Guangzhou Zhanshi Bao*, 7 December 2005. OSC ID CPP20060228380001.

McDevitt, Michael. *China's Naval Modernization: Cause for Storm Warnings?* The Institute for National Strategic Studies of the National Defense University, 16 June 2010.

McFadden, Frank E. and Richard D. Arnold. "Supply Chain Risk Mitigation for IT Electronics." *2010 IEEE Conference on Technologies for Homeland Security.* IEEE, 2010. <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5655094>.

Medeiros, Evan S., Roger Cliff, Keith Crane, and James C. Mulvenon. *A New Direction for China's Defense Industry.* RAND Corp., 2005.

Mellor, Chris. "Huawei-Symantec takes big step with Force10." *Channel Register,* 1 March 2011. <http://www.channelregister.co.uk/2011/03/01/huawei_symantec_force_ten/>.

Meng Fanjun. "Network-centric warfare: the American way of war in the information age," *National Defense and Armed Forces Building in the New and Century New Age*. Military Yiwen Press, 2008.

"Military Experts Share Views on 'Cyber Defense' and National Defense." *PLA Daily,* 6 January 2011. <http://english.pladaily.com.cn>.

Military Report. CCTV-7, Beijing. 22 October 2011 and 27 October 2011. Television. OSC ID FEA20111025023575.

Military Report. CCTV-7, Beijing. 27 September 2011. Television. OSC ID CPP20110927091001.

Ming Yi Business Consulting (Beijing). "*973 Jihua Zai Shiyi Wu Qijian De Zhidao Fangzhen*" (Program Guidelines in the Eleventh Five-Year Plan). <www.xiangmu010.com/973guidelines.html>. Viewed November 2011.

"Mobile 4G: China Mobile Rolling Out TD-LTE Trials." *GoMo News,* 4 January 2011. <http://www.gomonews.com/mobile-4g-china-mobile-rolling-out-td-lte-trials/>.

"More foundry competition means lower chip prices." digikey.com. Digi-Key Corporation, 27 September 2011. <http://www.digikey.com/purchasingpro/us/en/articles/buying-conditions/more-foundry-competition-means-lower-chip-prices/1210>.

Mulvenon, James and Rebecca Samm Tyroler-Cooper. "China's Defense Industry on the Path of Reform." U.S. China Economic and Security Review Commission, October 2009. <http://www.uscc.gov/researchpapers/2009/DGIReportonPRCDefenseIndustry--FinalVersion_10Nov2009.pdf>.

Mulvenon, James. "Chairman Hu and the PLA's 'New Historic Missions,'" *China Leadership Monitor* 27 (Winter 2009). <http://media.hoover.org/sites/default/files/documents/CLM27JM.pdf>.

Mulvenon, James. "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability." in Roy Kamphausen, David Lai, Andrew Scobell, eds. *Beyond the Strait: PLA Missions Other Than Taiwan.* Strategic Studies Institute, April 2009.

Nan Li. "The PLA's Evolving Campaign Doctrine and Strategies." in James C. Mulvenon, Richard H. Yang. *The People's Liberation Army in the Information Age*. Rand, 1999.

"The National Security Implications of Investments and Products from the People's Republic of China In The Telecommunications Sector." U.S.-China Economic and Security Review Commission, January 2011.

Nazario, Jose. "Politically Motivated Denial of Service Attacks." Arbor Networks, July 2009. <http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf>.

"Nokia Booklet 3G *Bianzhong Da Shang* TD-LTE *Yu Beijing Xianshen, Kexi Zhi Shi Ceshi Ji*" (Nokia Booklet 3G TD-LET Variant Appears in Beijing; Unfortunately, It Is Only a Test Device). Engadget, 27 September 2011. <http://cn.engadget.com/2011/09/27/nokia-booklet-td-lte-leaked-but-not-sell/>.

Northwest Polytechnical University. "*Jisuanji Xueyuan Xueke Fangxiang Jieshao*" (Introduction to the Computer Science Department). <www.nwpu.edu.cn>. Viewed November 2011.

Open Source Center. "Huawei Annual Report Details Directors, Supervisory Board for First Time." 5 October 2011. OSC ID FEA20111005022749.

Open Source Center. "PRC 2010 Military Training Aims at Strategic Campaigns, Longer Reach." 29 January 2010. OSC ID CPF20100129565001.

Oracle. "Datang Software Technologies Certifies Their Telecom Network Resource Management System on Oracle Database 11g and Oracle Real Application Clusters." May 2009. <http://www.oracle.com/us/products/database/datang-066595.pdf>.

Pan Chin-chang. "*Lun Gong Jun Zixun Hua Zhanzheng Zhi Xinli Zhan*" (On the Role of Psychological Warfare as a Part of the PLA's Informatized Warfare Operations). *Army Studies Bimonthly* 43 492 (April 2007). OSC ID CPP20071119312002.

Paul, Ryan. "Researchers Identify Command Servers Behind Google Attack." *Ars Technica*, January 2010. <http://www.arstechnical.com/security/news/2010/01/researchers-identify-command-servers-behind-google-attack.ars>.

Peng Guangqiang and Yao Youzhi, eds. *The Science of Military Strategy.* Military Science Publishing House, English Edition, 2005.

"Persist in Taking the Scientific Development as Guidance—Second Commentary on Education Activities on Chinese Military's Loyal Fulfillment of Historic Missions in the New Century and New Stage," *PLA Daily*, 27 March 2006.

Philpott, Don, ed., *A Guide to Federal Terms and Acronyms* (2011).

"PLA Reinforces Information and Electronic Warfare Capability." *Kanwa Asian Defence*, February 2010. <http://www.kanwa.com/dnws/showpl.php?id=540>.

Pollpeter, Kevin et. al. *Seizing the Ultimate High Ground: Chinese Military Writings on Space and Counterspace.* Center for Intelligence Research and Analysis, April 2009.

Pope, Sydney, Brian S. Cohen, Vashisht Sharma, Ryan R. Wagner, Loren W. Linholm and Sherry Gillespie. "Verifying Trust For Defense Use Commercial Semiconductors." Office of the Secretary of Defense, March 2010. <http://www.acq.osd.mil/mibp/docs/Verifying_Trust_for_Defense_Use_Commercial_Seminconductors.pdf>.

PRC Ministry of Industry and Information Technology. "Military-Civilian Promotion Division." <http://jmjhs.miit.gov.cn/n11293472/n11295/index.html>. Viewed November 2011.

PRC Ministry of Industry and Information Technology. "*Zhejiang Sheng Chenggong Juban Junmin Liangyong Jishu Hezuo Duijie Hui*" (Zhejiang Province Successfully Holds Dual-Use Technology Cooperation Matchmaking). 17 October 2011. <http://jmjhs.miit.gov.cn/n11293472/n11295193/n11298598/14276272.html>.

PRC Ministry of Public Security. "Ministry of Public Security Named its First Ministerial Key Laboratories." 12 September 2008. <http://www.mps.gov.cn/n16/n2130130/index.html>.

PRC Ministry of Science and Technology. "*Guanyu Zhengji Shi'er Wu 863 Jihua Gaoxiao Neng Jisuanji Ji Yingyong Fuwu Huanjing Zhongda Xiangmu Keti Jianyi De Tongzhi*" (Notice Concerning a Call for 12th Five-Year Program 863 Program Major Projects on High-Performance Computing and Application Server Environments). <www.zjsb.org/List.asp?ID=2370>. Viewed November 2011.

PRC Ministry of Science and Technology. "*Guojia Gao Jishu Yanjiu Fazhan Jihua (863 Jihua)*" (The National High-Tech Research and Development Program). <www.863.gov.cn>. Viewed November 2011.

PRC Ministry of Science and Technology. "*Guojia Zhongdian Jichu Yanjiu Fazhan Jihua*" (The National Key Basic Research Program). <www.973.gov.cn>. Viewed November 2011.

PRC Ministry of Science and Technology. "*Yiti Hua Kexin Wangluo Yu Pushi Fuwu Tixi Jichu Yanjiu*" (Basic Research in Integrated Trusted Networks and Universal Service Systems). <www.973.gov.cn>. Viewed November 2011.

PRC National Bureau of Statistics. "*Di Er Ci Quanguo Kexue Yanjiu Yu Shiyan Fazhan (R&D) Ziyuan Qingcha*" (Second National Scientific Research and Development Resource Inventory No. 3). 22 November 2010. <http://www.stats.gov.cn/tjgb/rdpcgb/qgrdpcgb/t20101122_402684878.htm>.

PRC National Development and Reform Commission. "*Gonggao*" (Notice). <http://www.ndrc.gov.cn/zcfb/zcfbgg/2008gonggao/t20080530_215271.htm>. Viewed November 2011.

PRC National University of Defense Technology. "*Jichu Yanjiu Zhongdian Yanjiu Lingyu He Fangxiang*" (Areas and Directions of Basic and Key Research) and "*Zhuyao Yanjiu Fangxiang*" (Main Research Directions). <www.nudt.edu.cn/intrdouce.asp?classid=250> [sic]. Viewed November 2011.

PRC State Council. "*Gongye He Xinxi Hua Bu Zhuyao Zhize Nei She Jigou He Renyuan Bianzhi Guiding Yinfa*" (Issuance Concerning the Major Internal Organization and Staffing Responsibilities of the Ministry of Industry and Information Technology). 11 July 2008. <http://www.miit.gov.cn>.

Qi Lao Hu Yao Fawei ("Autumn Tiger"). "*Shanghai Jiao Tong Daxue Jisuanji Xi Kejiu Renyuan Jiufa Wangluo Zhanzheng Duikang Moni Danyuan*" (Shanghai Jiao Tong University Department of Computer Science and Engineering Researchers Develop Network Warfare

Countermeasures Simulation Module). 3 September 2011. <http://blog.sina.com.cn/s/blog_8d1b66e0100y5vn.html>.

Ragan, Steve. "RSA's 'Trial by Fire' Caused by Two State-Sponsored Groups." *Security Week,* 12 October 2011. <www.securityweek.com/rsas-trial-fire-caused-two-state-sponsored-groups>.

"Rootkits on Cisco IOS Devices." Cisco, 16 May 2008. <http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20080516-rootkits>.

"Samsung lags in foundry rankings." eetimes.com. EE Times, 20 January 2011. <http://www.eetimes.com/electronics-news/4212366/Samsung-lags-in-foundry-rankings->.

Shanghai Jiao Tong University. "Cryptography and Information Security." <www.cs.sjtu.edu.cn>. Viewed November 2011.

Shanghai Jiao Tong University. "*Datang Dianxin Jituan Lai Wo Xiao Jinxing Xiao Qi Hezuo Diaoyan*" (Datang Telecom Group to Visit, Will Conduct Academic-Commercial Cooperative Research). 8 November 2010. <kejichu.sjtu.edu.cn/info/news/nry/5823.htm>.

Shanghai Jiao Tong University. "GU Dawu." <www.cs.sjtu.edu.cn/people_detail.action?id=4>. Viewed November 2011.

Shanghai Jiao Tong University. "Zheng Dong." <cis.sjtu.edu.cn/personal/zhengdong/zhengdong.htm>. Viewed November 2011.

"Shenyang MR Units Use 'Blue Force' To Strengthen Informatized Operations." *Qianjin Bao*, 6 May 2008. OSC ID CPP20080623318001.

"*Shi Nian Gao Jiaohui Junmin Keji Jie Shuoguo*" (10th Annual Exhibition: Dual-Use Science and Technology). Chongqing Civilization Network, 8 July 2010. <http://cq.wenming.cn/jrcq/201007/t20100708_12010.htm>.

"Slip-Up in Chinese Military TV Show Reveals More Than Intended." *The Epoch Times*, 21 August 2011. <http://www.theepochtimes.com/n2/china-news/slip-up-in-chinese-military-tv-show-reveals-more-than-intended-60619.html>.

sourcexperts.com. "Datang Software Technologies, Ltd." 19 January 2005. <http://www.sourceexperts.com/outsourcing.cfm/directory.profile/company/datang-software-technologies-ltd/pid/144310>.

Southeast University. "*Guanyu Yinfa 'Dongnan Daxue 2010 Nian Biye Yanjiusheng Jiuye Banfa' He 'Dongnan Daxue 2010 Jie Benke Biye Sheng Jiuye Banfa' De Tongzhi*" (Notice Concerning "Job Placement for Southeast University's 2010 Graduate Students" and "Job Placement for Southeast University's 2010 Undergraduate Students"). 2009. <www.seu.edu.cn>.

Springut, Micah, Steven Schlaikjer, and David Chen. "China's Program for Science and Technology Modernization: Implications for American Competitiveness." U.S.-China Economic and Security Review Commission, January 2011. <http://www.uscc.gov/researchpapers/2011/USCC_REPORT_China%27s_Program_forScience_and_Technology_Modernization.pdf>.

Fraser, William. "Hearing on U.S. Pacific Command and U.S. Transportation Command in review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program." Senate Armed Services Committee. Dirksen Senate Office Building, Washington, D.C., 28 February 2012. Testimony. http://armed-services.senate.gov/Transcripts/2012/02 February/12-04 - 2-28-12.pdf

Stokes, Mark, Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Project 2049 Institute, 11 November 2011.

Stokes, Mark. "China's Evolving Conventional Strategic Strike Capability." Project 2049 Institute, 14 September 2009. <http://project2049.net/documents/chinese_anti_ship_ballistic_missile_asbm.pdf>.

Stokes, Mark. "China's Strategic Modernization: Implications for the United States." U.S. Army Strategic Studies Institute (1999).

Stokes, Mark, Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Project 2049 Institute (November 11, 2011).

"Strategic cooperation with Datang for mobile technology development in China." Ericsson, 20 April 2010. <http://www.ericsson.com/thecompany/press/releases/2010/04/1405884>.

Sun Xiaoyan, Wu Dongying, Zhu Yuefei, and Guo Ning. "Research and Improvement of Wu-Manber Multi-pattern Matching Algorithm," *Jisuanji Gongcheng* (Computer Engineering) (1 April 2008).

Supply Chain Risk Management (SCRM). Information Technology Lab, National Institute of Standards and Technology, 25 January 2012. <http://csrc.nist.gov/scrm/>.

Swanson, Marianne, Nadya Bartol, and Rama Moorth. "Piloting Supply Chain Risk Management Practices For Federal Information Systems (NISTIR 7622)." National Institute of Standards and Technology, June 2010.

Tai Ming Cheung. *Fortifying China: The Struggle to Build a Modern Defense Economy*. Cornell University Press, 2009.

Tang Jun et al. "Simulation Study on Worm Propagation Characteristics." *Xitong Fangzhen Xuebao,* 9 December 2010.

Tang Xiaohua and Geng Dexing. "Study Of Hu Jintao's Important Explications On Development Of National Defense And Armed Forces." *China Military Studies* 75 (Spring 2010).

Tianya BBS. "*[Xi'an] Xinren Qiuzhu, Guanyu Dianxin Kexue Jishu Di Shi Yanjiu Suo (Youdian Shi Suo)*" ([Xi'an] Newbie help request about MIIT 10th Research Institute (Posts and Telecoms 10th Institute). 1 March 2010. <http://bbs.city.tianya.cn/new/tianyacity/content.asp?idWriter=0&Key=0&idItem=266&idArticle=58297&page_num=1>.

Tsai, Ching-Jung and Wang, Jenn-hwang. "How China institutional changes influence industry development? The case of TD-SCDMA industrialization." Druid Society, June 2011. <druid8.sit.aau.dk/acc_papers/7gx623ot4yrtcldt7yjked2chd3.pdf>.

"TSMC First Pure-Play Foundry to Join Top-10 R&D Spenders." IC Insights Research Bulletin, 13 January 2011. <http://www.icinsights.com/data/articles/documents/205.pdf>.

"Unidentified Yunnan-Based Artillery Regiment Diligently Seeks New Growth Points of Combat Power—Soft Kill Training Leyden, John. "RSA Defends Handling Of Two-Pronged SecurId Breach." *The Register,* 11 October 2011. <http://www.theregister.co.uk/2011/10/11/rsa_securid_breach_keynote/>.

University of Tennessee Chattanooga. "UTC SimCenter: National Center for Computational Engineering." <http://www.utc.edu/Research/SimCenter>. Viewed November 2011.

U.S. Commercial Service, American Consulate General Guangzhou. "South China Snapshot: Electronic Telecommunication Components." 2010. <http://export.gov/china/static/Telecom_Latest_eg_cn_025567.pdf>.

U.S. Department of Defense. "PLA Activities Report 01-15 Apr 2011." 13 May 2011. OSC ID CPP20110513563002.

U.S. Department of Defense. "PLA Activities Report 01-15 Oct 2009." 13 November 2009. OSC ID CPP20091113563001.

U.S. Department of Justice. "Departments of Justice and Homeland Security Announce 30 Convictions, More Than $143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware." May 2010. <http://www.justice.gov/opa/pr/2010/May/10-crm-534.html>.

U.S. Deputy Secretary of Defense. Report Number DTM 09-016, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems." 25 March 2010. <http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-016.pdf >.

U.S. Federal Bureau of Investigation. "United States District Court—District of Connecticut - No. 3:11 CV 561(VLB)." 11 April 2011. <http://www.fbi.gov/newhaven/press-releases/pdf/nh041311_4.pdf>.

U.S. National Security Agency. Report Number C4-040R-02, "Router Security Configuration Guide." 15 December 2005. <www.nsa.gov>.

U.S. Office of the Secretary of Defense. "Annual Report to Congress: Military and Security Development Regarding the People's Republic of China," 2010.

U.S. Transportation Command. "Instruction 10-25 Operations: Aerial Refueling." 6 May 2011.

"U.S.-based Companies Held 13 of the Top 20 Fabless Spots in 2010." IC Insights Research Bulletin, 21 April 2011. <http://www.icinsights.com/data/articles/documents/263.pdf>.

US-China Business Council. "2011 Special 301 Review." 15 February 2011. <https://www.uschina.org/public/documents/2011/ustr_special_301_review.pdf>

Villasenor, John. "The Hacker in Your Hardware." *Scientific American,* August 2010.

Walsh, Larry. "Symantec Will Continue to Partner with Huawei." Channelnomics, 17 November 2011. <http://channelnomics.com/2011/11/17/symantec-continue-partner-huawei/>

Wang Baocun. "An Exploratory Analysis of Chief Information Officer Systems In Foreign Militaries." National Defense and Armed Forces Building in the New and Century New Age. Military Yiwen Press, 2008.

Wang Fanhua. "The First State Secrecy Academy in Western China Established at Northwestern Polytechnical University." Northwest Polytechnical University, 12 January 2011.

Wang Jian-Wei and Li-Li Rong. "Cascade-Based Attack Vulnerability on the U.S. Power Grid." *Safety Science* 47 (February 2009).

Wang Jian-Wei and Li-Li Rong. "Edge-based Attack induced Cascading Failures On Scale-Free Networks." *Physica A: Journal of Statistical Mechanics and its Applications* 388 (2009).

Wang Jixiang, Liu Guizhong, and Feng Ying. "Evaluation of Jamming Effect of AM Communications Based on Modulation and Recognition Features." *Junshi Yunchou Yu Xitong Gongcheng* (Military Operations Research and Systems Engineering) 24, 2: 75-78.

Wang Xiaoming. "Explorative Study of Laws in Developing Capabilities for Information System-Based System-of-Systems Operations." *China Military Science* 1-2011 (February 2011).

Wang Zhengde, Yang Shisong and Zhou Lin, eds. *Xinxi Duikang Lilun* (Information Confrontation Theory). PLA Information Engineering University/ Military Science Publishing House, 2007.

Wheeler, D. and G. Larsen. "Planning For the Future of Cyber Attack Attribution." House of Representatives Subcommittee on Technology and Innovation, Committee on Science and Technology, 15 July 2010. <http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg57603/html/CHRG-111hhrg57603.htm>.

Wiencek, David G. "South China Sea Flashpoint." The Jamestown Foundation, 24 July 2001. <http://www.jamestown.org/single/?tx_ttnews[tt_news]=28452>.

Wo Jieming. "Faithfully Carry out the Military's Historic Mission-100 Questions and Answers" (*Zhongshi Luxing Xin Shiji Xin Jieduan Wojun Lishi Shiming Bai Wen Bai Da*"). Changzheng Publishing, 1 May 2006. OSC ID CPP20081022325003001.

Wu Dilun et al. "General Staff Department Lays Out Plan for Military Training Throughout the Armed Forces in the New Year." *PLA Daily*, 7 January 2009. OSC ID CPP20090107710002.
Wu Tianmin. "2010: Military Training of the Three Services To Be Further Promoted." *PLA Daily*, 8 January 2010. OSC ID CPP20100108710005.

Xi'an Jiao Tong University. "*Guanyu Shenbao Guojia 242 Xinxi Anquan Jihua Xiangmu De Tongzhi*" (Notice Concerning Reports of the National 242 Information Security Program). June 2006. <std.xjtu.edu.cn/html/xinxi/2006/06/11089.html>.

Xiang Sibing and Li Dajun. "Analysis of Russian military information warfare theory." National Defense and Armed Forces Building in the New Century and New Age. Military Yiwen Press, 2008.

Xie Youlin. "*Zhonggong Tanhuan Zhan Siwei Yu Zhan Li Fazhan Yanxi*" (Study, Analysis of Communist Party of China's Paralysis Warfare, Thought, Combat Force Development). *National Defense Journal* 24 2 (1 April 2009). OSC ID CPP20100414312004.

Xu Changdu and Zhang Zhidong. "High-Tech Militia Detachments Cannot Become 'Militia Detachments on Display,'" *Renmin Qianxian,* 25 March 2005. OSC ID CPP20050606000179.

LTC Yan Zhensheng, MAJ Liu Haijing, and MAJ Feng Wei. "On Composition And Basic Mode Of Generating Information-System-Based System Of Systems Operational Capabilities." *China Military Science* 4 (2010). OSC ID CPP20101208563001.

Yang Baoming, Zhao Changjun, and Xu Jianhua. "Dialectical Considerations On Operation Guidance Under Informatized Conditions." *China Military Science* 4 (2010). OSC ID CPP20101210563001.

Yang Huicheng. "PLA Daily Learns From the Military Training and Arms Department under the PLA General Staff Department that a New Upsurge in Military Training Will Be Initiated in All PLA Troops in 2006." *PLA Daily,* 3 January 2006. OSC ID CPP20060103510001.

Ye Youcai and Zhou Wenrui. "Building a High-quality Militia Information Technology Element." *Guofang* (National Defense), 15 September 2003.

Ye Zheng and Zhao Baoxian. "How Do You Fight a Network War?" *Zhongguo Qingnian Bao,* 3 June 2011. OSC ID CPP20110603787004.

Zetter, Mark. "Economic drivers, challenges creating regional electronics industry." Venture Outsource, December 2009. <http://www.ventureoutsource.com/contract-manufacturing/benchmarks-best-practices/executive-management/economic-drivers-challenges-creating-regional-electronics->.

Zhang Hong and Yu Zhao. "Forge New Type of Operational Force Capability System Based on Information System." *China Military Science* 5-2010 (2010).

Zhang Yang. "Opening Up Rich Soil at the Front Lines to Nurture Talent." *PLA Daily*, 1 February 2009.