Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation

Prepared for

The US-China Economic and Security Review Commission

Project Manager
Steve DeWeese 703.556.1086 steve.deweese@ngc.com

Principal Author
Bryan Krekel

Subject Matter Experts
George Bakos
Christopher Barnett

Northrop Grumman Corporation
Information Systems Sector
7575 Colshire Drive
McLean, VA 22102

October 9, 2009

NORTHROP GRUMMAN

Table of Contents

Scope Note

This paper presents a comprehensive open source assessment of China's capability to conduct computer network operations (CNO) both during peacetime and periods of conflict. The result will hopefully serve as useful reference to policymakers, China specialists, and information operations professionals. The research for this project encompassed five broad categories to show how the People's Republic of China (PRC) is pursuing computer network operations (CNO) and the extent to which it is being implemented by examining:

a) The PLA's strategy for computer network operations at the campaign and strategic level to understand how China is integrating this capability into overall planning efforts and operationalizing it among its field units;

b) Who are the principal institutional and individual "actors" in Chinese CNO and what linkages may exist between the civilian and military operators;

c) Possible targets of Chinese CNO against the US during a conflict to understand how the PLA might attempt to seize information control over the US or similar technologically advanced military during a conflict;

d) The characteristics of ongoing network exploitation activities targeting the US Government and private sector that are frequently attributed to China;

e) A timeline of alleged Chinese intrusions into US government and industry networks to provide broader context for these activities.

The basis for this work was a close review of authoritative open source PLA writings, interviews with Western PLA and information warfare analysts, reviews of Western scholarship on these subjects, and forensic analysis of intrusions into US networks assessed to have Chinese origins. The research draws heavily from journals and articles published by the Chinese National Defense University and the Academy of Military Sciences, the military's highest authority for issues of doctrine, strategy, and force modernization. Many of these publications offer substantive insights into current thinking on strategy and doctrinal issues related to information warfare and CNO. Additional insights into the role of information warfare in broader campaign doctrine and strategy came from *The Science of Military Strategy, The Science of Campaigns*, two of the most authoritative sources on the subject available in the open press. The military's official newspaper, *The PLA Daily*, and a range of Chinese military journals, official media, provincial and local media as well as non-PRC regional media, all provided data on information warfare (IW) training events.

Technical assessments of operational tradecraft observed in intrusions attributed to China are the result of extensive forensic analysis and discussions with information security professionals who follow these issues closely. A review of Chinese technical journal articles on computer network attack and exploitation techniques also aided this study. This research was obtained from online Chinese databases accessible in the US.

A regular review of the contents and discussions posted on Chinese hacker Websites contributed to the analysis of these groups' activities and capabilities. The focus of this effort was to identify possible interactions between members of these groups and the government. Conversations with Western information security analysts who closely follow these groups and actors contributed immensely to focusing the research and greatly aided our understanding of China's hacker communities.

This study was not scoped to include research in China, consequently, the authors focused on the materials and insights presently available outside of China. Additional in-country research on this subject is an avenue of future effort that can—and should—supplement the work presented here.

Executive Summary

The government of the People's Republic of China (PRC) is a decade into a sweeping military modernization program that has fundamentally transformed its ability to fight high tech wars. The Chinese military, using increasingly networked forces capable of communicating across service arms and among all echelons of command, is pushing beyond its traditional missions focused on Taiwan and toward a more regional defense posture. This modernization effort, known as informationization, is guided by the doctrine of fighting "Local War Under Informationized Conditions," which refers to the PLA's ongoing effort to develop a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum.

This doctrinal focus is providing the impetus for the development of an advanced IW capability, the stated goal of which is to establish control of an adversary's information flow and maintain dominance in the battlespace. Increasingly, Chinese military strategists have come to view information dominance as the precursor for overall success in a conflict. The growing importance of IW to China's People's Liberation Army (PLA) is also driving it to develop more comprehensive computer network exploitation (CNE) techniques to support strategic intelligence collection objectives and to lay the foundation for success in potential future conflicts.

One of the chief strategies driving the process of informatization in the PLA is the coordinated use of CNO, electronic warfare (EW), and kinetic strikes designed to strike an enemy's networked information systems, creating "blind spots" that various PLA forces could exploit at predetermined times or as the tactical situation warranted. Attacks on vital targets such as an adversary's intelligence, surveillance, and reconnaissance (ISR) systems will be largely the responsibility of EW and counterspace forces with an array of increasingly sophisticated jamming systems and anti-satellite (ASAT) weapons. Attacks on an adversary's data and networks will likely be the responsibility of dedicated computer network attack and exploitation units.

The Chinese have adopted a formal IW strategy called "Integrated Network Electronic Warfare" (INEW) that consolidates the offensive mission for both computer network attack (CNA) and EW under PLA General Staff Department's (GSD) 4th Department (Electronic Countermeasures)[1] while the computer network defense (CND) and

[1] The General Staff Department is the highest organizational authority in the PLA responsible for the daily administrative duties of the military. It is comprised of seven functional departments: operations, intelligence, signals intelligence, electronic countermeasures, communications, mobilization, foreign relations, and management.

intelligence gathering responsibilities likely belong to the GSD 3rd Department (Signals Intelligence), and possibly a variety of the PLA's specialized IW militia units.

This strategy, which relies on a simultaneous application of electronic warfare and computer network operations against an adversary's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks and other essential information systems, appears to be the foundation for Chinese offensive IW. Analysis of this strategy suggests that CNO tools will be widely employed in the earliest phases of a conflict, and possibly preemptively against an enemy's information systems and C4ISR systems.

The PLA is training and equipping its force to use a variety of IW tools for intelligence gathering and to establish information dominance over its adversaries during a conflict. PLA campaign doctrine identifies the early establishment of information dominance over an enemy as one of the highest operational priorities in a conflict; INEW appears designed to support this objective.

The PLA is reaching out across a wide swath of Chinese civilian sector to meet the intensive personnel requirements necessary to support its burgeoning IW capabilities, incorporating people with specialized skills from commercial industry, academia, and possibly select elements of China's hacker community. Little evidence exists in open sources to establish firm ties between the PLA and China's hacker community, however, research did uncover limited cases of apparent collaboration between more elite individual hackers and the PRC's civilian security services. The caveat to this is that amplifying details are extremely limited and these relationships are difficult to corroborate.

China is likely using its maturing computer network exploitation capability to support intelligence collection against the US Government and industry by conducting a long term, sophisticated, computer network exploitation campaign. The problem is characterized by disciplined, standardized operations, sophisticated techniques, access to high-end software development resources, a deep knowledge of the targeted networks, and an ability to sustain activities inside targeted networks, sometimes over a period of months.

Analysis of these intrusions is yielding increasing evidence that the intruders are turning to Chinese "black hat" programmers (i.e. individuals who support illegal hacking activities) for customized tools that exploit vulnerabilities in software that vendors have not yet discovered. This type of attack is known as a "zero day exploit" (or "0-day") as the defenders haven't yet started counting the days since the release of vulnerability information. Although these relationships do not prove any government affiliation, it suggests that the individuals participating in ongoing penetrations of US networks have Chinese language skills and have well established

ties with the Chinese underground hacker community. Alternately, it may imply that the individuals targeting US networks have access to a well resourced infrastructure that is able to broker these relationships with the Chinese blackhat hacker community and provide tool development support often while an operation is underway.

The depth of resources necessary to sustain the scope of computer network exploitation targeting the US and many countries around the world coupled with the extremely focused targeting of defense engineering data, US military operational information, and China-related policy information is beyond the capabilities or profile of virtually all organized cybercriminal enterprises and is difficult at best without some type of state-sponsorship.

The type of information often targeted for exfiltration has no inherent monetary value to cybercriminals like credit card numbers or bank account information. If the stolen information is being brokered to interested countries by a third party, the activity can still technically be considered "state-sponsored," regardless of the affiliation of the actual operators at the keyboard.

The US information targeted to date could potentially benefit a nation-state defense industry, space program, selected civilian high technology industries, foreign policymakers interested in US leadership thinking on key China issues, and foreign military planners building an intelligence picture of US defense networks, logistics, and related military capabilities that could be exploited during a crisis. The breadth of targets and range of potential "customers" of this data suggests the existence of a collection management infrastructure or other oversight to effectively control the range of activities underway, sometimes nearly simultaneously.

In a conflict with the US, China will likely use its CNO capabilities to attack select nodes on the military's Non-classified Internet Protocol Router Network (NIPRNET) and unclassified DoD and civilian contractor logistics networks in the continental US (CONUS) and allied countries in the Asia-Pacific region. The stated goal in targeting these systems is to delay US deployments and impact combat effectiveness of troops already in theater.

No authoritative PLA open source document identifies the specific criteria for employing computer network attack against an adversary or what types of CNO actions PRC leaders believe constitutes an act of war.

Ultimately, the only distinction between computer network exploitation and attack is the intent of the operator at the keyboard: The skill sets needed to penetrate a network for intelligence gathering purposes in peacetime are the same skills necessary to penetrate that network for offensive action during wartime. The difference is what the operator at that keyboard does with (or *to*) the information once

inside the targeted network. If Chinese operators are, indeed, responsible for even some of the current exploitation efforts targeting US Government and commercial networks, then they may have already demonstrated that they possess a mature and operationally proficient CNO capability.

Chinese Computer Network Operations Strategy

The Chinese People's Liberation Army (PLA) is actively developing a capability for computer network operations (CNO) and is creating the strategic guidance, tools and trained personnel necessary to employ it in support of traditional warfighting disciplines. Nonetheless, the PLA has not openly published a CNO strategy with the formal vetting of the Central Military Commission (CMC), China's top military decisionmaking body, or the Academy of Military Sciences (AMS), its leading body for doctrine and strategy development . The PLA has however, developed a strategy called "Integrated Network Electronic Warfare" that is guiding the employment of CNO and related information warfare tools. The strategy is characterized by the combined employment of network warfare tools and electronic warfare weapons against an adversary's information systems in the early phases of a conflict.

Chinese information warfare strategy is closely aligned with the PLA's doctrine for fighting Local Wars Under Informationized Conditions, the current doctrine that seeks to develop a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum. China's military has shifted from a reliance on massed armies of the Maoist Era People's War doctrine and is becoming a fully mechanized force linked by advanced C4ISR technologies.

Informationization is essentially a hybrid development process, continuing the trend of mechanization and retaining much of the current force structure while overlaying advanced information systems on it to create a fully networked command and control (C2) infrastructure.[2] The concept allows the PLA to network its existing force structure without radically revising current acquisition strategies or order of battle.

- PLA assessments of current and future conflicts note that campaigns will be conducted in all domains simultaneously—ground, air, sea, and electromagnetic—but it is the focus of the latter domain in particular that has driven the PLA's adoption of the Informationized Conditions doctrine.[3]

[2] *China's National Defense in 2008,* Information Office of the State Council of the People's Republic of China, Beijing, 29 December 2008. http://www.chinadaily.com.cn/china/2009-01/20/content_74133294.htm

[3] *China's National Defense in 2004,* Information Office of the State Council of the People's Republic of China, Beijing, 27 December 2004, available at: http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html | *China's National Defense in 2006,* Information Office of the State Council of the People's Republic of China, Beijing, 29 December 2006, available at http://english.chinamil.com.cn/site2/news-channels/2006-12/29/content_691844.htm

This doctrine is also influencing how the PLA approaches its military campaigns, attempting to shift from the traditional combined arms operations to what the PLA refers to as "integrated joint operations under informationized conditions." The former is characterized by large mechanized formations fighting in tandem but without a shared common operating picture and the latter stresses the dominance of information technology and its ability to shape ground, sea, air, and space into a multi-dimensional battlefield. In the integrated joint operations framework, the PLA uses information network technology to connect its services and warfighting disciplines into an integrated operational whole, a concept that is also shaping the PLA's approach to information warfare.

Achieving information dominance is one of the key goals for the PLA at the strategic and campaign level, according to The Science of Military Strategy and The Science of Campaigns, two of the PLA's most authoritative public statements on its doctrine for military operations.[4] Seizing control of an adversary's information flow and establishing information dominance (*zhi xinxi quan*) are essential requirements in the PLA's campaign strategy and are considered so fundamental that *The Science of Military Strategy* considers them a prerequisite for seizing air and naval superiority.[5]

- *The Science of Military Strategy* and *The Science of Campaigns* both identify enemy C4ISR and logistics systems networks as the highest priority for IW attacks, which may guide targeting decisions against the US or other technologically advanced opponents during a conflict.

- *The Science of Campaigns* states that IW must mark the start of a campaign and, used properly, can enable overall operational success.[6]

The seeming urgency in making the transition from a mechanized to an informationized force is driven by the perception that winning local wars against adversaries with greater technological advantages, such as the United States, may not be possible without a strong information warfare capability to first control enemy access to its own information.[7]

---

[4] Wang Houqing and Zhang Xingye, chief editors, *The Science of Campaigns*, Beijing, National Defense University Press, May 2000. See chapter six, section one for an overview of information warfare in campaign settings. | Peng Guangqiang and Yao Youzhi, eds, *The Science of Military Strategy*, Military Science Publishing House, English edition, 2005, p. 338
[5] Peng and Yao, p. 336.
[6] OSC, CPP20010125000044, "Science of Campaigns, Chapter 6, Section 1," 1 May 2000
[7] OSC, CPP20081112563002, "On the Trend of Changes in Operations Theory Under Informatized Conditions," by Li Zhilin, *China Military Science,* Winter 2008; | OSC,

- PLA discussions of information dominance focus on attacking an adversary's C4ISR infrastructure to prevent or disrupt the acquisition, processing, or transmission of information in support of decisionmaking or combat operations. The goal is to combine these paralyzing strikes on the command and control architecture with possible hard kill options using missiles, air strikes, or Special Forces against installations or hardware.

- Degrading these networks potentially prevents the enemy from collecting, processing, and disseminating information or accessing information necessary to sustain combat operations, allowing PLA forces to achieve operational objectives such as landing troops on Taiwan in a cross-strait scenario before the US can effectively intervene.

The PLA has also come to recognize the importance of controlling space-based information assets as a means of achieving true information dominance, calling it the "new strategic high ground," and many of its advocates consider space warfare to be a subset of information warfare.[8] The PLA is seeking to develop the capability to use space for military operations while denying this same capability to an adversary. PLA authors acknowledge that space dominance is also essential for operating joint campaigns and for maintaining the initiative on the battlefield. Conversely, they view the denial of an adversary's space systems as an essential component of information warfare and a prerequisite for victory. [9]

The PLA maintains a strong R&D focus on counterspace weapons and though many of the capabilities currently under development exceed purely cyber or EW options, they are nonetheless, still considered "information warfare" weapons.[10] Among the most high profile of China's ASAT capabilities are kinetic weapons, which rely on projectiles or warheads fired at high speed to impact a satellite directly. The successful January 2007 test of this capability against a defunct Chinese weather satellite demonstrated that the PLA has moved past theoretical discussions of this option and toward an operational capability. Directed energy weapons, such as lasers, high power microwave systems and nuclear generated electromagnetic pulse

---

CPP20081028682007, "A Study of the Basic Characteristics of the Modes of Thinking in Informatized Warfare," by Li Deyi, *China Military Science*, Summer 2007.

[8] Dean Cheng, *PLA Views on Space: The Prerequisite for Information Dominance," Center for Naval Analysis*, CME D0016978.A1, October 2007, p. 7

[9] Integrated Air, Space-Based Strikes Vital in Informatized Warfare | OSC, CPP20081014563001, "On the Development of Military Space Power," China Military Science, March 2008

[10] OSC, CPP20080123572009, "PRC S&T: Concept of Kinetic Orbit Weapons and Their Development," Modern Defense Technology*,* 1 Apr 05

attacks (EMP), are under development. The perceived benefits are the immediacy, and in the case of EMP, the broad scope of the effect.[11]

While the use of any of these weapons against US satellites could quickly escalate a crisis, detonating a nuclear device to create an EMP effect runs an especially high risk of crossing US "red lines" for the definition of a nuclear attack, even if the attack is carried out in the upper reaches of the atmosphere. Additionally, EMP is non-discriminatory in its targeting and though the PLA is training and preparing its force to operate under "complex electromagnetic conditions," many of its own space-based and possibly terrestrial communications systems may be damaged by either high altitude or more localized EMP attacks. At a minimum, EMP and other types of ASAT attacks expose the PLA to retaliatory strikes against China's own burgeoning satellite constellation, potentially crippling its nascent space-based C4ISR architecture.

A full discussion of Chinese capabilities for space information warfare is beyond the scope of the present study's focus on computer network operations, however, the subject is becoming central to the PLA's discussions of information warfare and in its analysis of informationization in the Chinese force structure.

Integrated Network Electronic Warfare

The conceptual framework currently guiding PLA IW strategy is called "Integrated Network Electronic Warfare" (*wangdian yitizhan*) a combined application of computer network operations and electronic warfare used in a coordinated or simultaneous attack on enemy C4ISR networks and other key information systems. The objective is to deny an enemy access to information essential for continued combat operations. ***The adoption of this strategy suggests that the PLA is developing specific roles for CNO during wartime and possibly peacetime as well.***

- PLA campaign strategy also reflects an intention to integrate CNO and EW into the overall operational plan, striking enemy information sensors and networks first to seize information dominance, likely before other forces engage in combat.

- The INEW strategy relies on EW to jam, deceive, and suppress the enemy's information acquisition, processing, and dissemination capabilities; CNA is

[11] Kevin Pollpeter, Leah Caprice, Robert Forte, Ed Francis, Alison Peet, *Seizing the Ultimate High Ground: Chinese Military Writings on Space and Counterspace,* Center for Intelligence Research and Analysis, April 2009, p. 32.

intended to sabotage information processing to "attack the enemy's perceptions."[12]

Consistent references to various elements of INEW by PLA authors in authoritative publications strongly suggest that the PLA has adopted it as its dominant IW strategy, despite the apparent lack of any publicly available materials indicating that the principle has received official vetting from senior PLA leaders.

- The originator of the INEW strategy, Major General Dai Qingmin, a prolific and outspoken supporter of modernizing the PLA's IW capabilities, first described the combined use of network and electronic warfare to seize control of the electromagnetic spectrum as early as 1999 in articles and a book entitled *An Introduction to Information Warfare,* written while on faculty at the PLA's Electronic Engineering Academy.[13]

- An uncorroborated Taiwan media source claims that Major General Dai drafted a 2002 internal PLA report stating that the PLA adopted an IW strategy using integrated network and electronic warfare as its core.[14]

- A July 2008 analysis of PLA information security architecture requirements by a researcher from the Second Artillery College of Engineering in Xian noted that "electronic warfare and computer network warfare are the two primary modes of attack in information warfare….By using a combination of electronic warfare and computer network warfare, i.e., "integrated network and electronic warfare," enemy information systems can be totally destroyed or paralyzed."[15]

- A 2009 source offered what may be the most succinct illustration of how INEW might be employed on the battlefield, stating that INEW includes "using techniques such as electronic jamming, electronic deception and suppression to disrupt information acquisition and information transfer, launching a virus attack or hacking to sabotage information processing and information utilization, and using anti-radiation and other weapons based on new mechanisms to destroy enemy information platforms and information facilities."[16]

---

[12] OSC, CPP20020624000214, "On Integrating Network Warfare and Electronic Warfare," *China Military Science*, Academy of Military Science, Winter 2002

[13] OSC, FTS20000105000705, "Fu Quanyou Commends New Army Book on IW," *PLA Daily*, 7 December 1999.

[14] OSC, CPP20071023318001, "Taiwan Military Magazine on PRC Military Net Force, Internet Controls," *Ch'uan-Ch'iu Fang-Wei Tsa-Chih* 1 March 2007.

[15] OSC, CPP20090528670007, "PRC S&T: Constructing PLA Information System Security Architecture, *Computer Security, (Jisuanji Anquan*), 1 Feb 2009.

[16] OSC, CPP20090528670007, "PRC S&T: Constructing PLA Information System Security Architecture, *Computer Security, (Jisuanji Anquan*), 1 Feb 2009.

In 2002, Dai published *An Introduction to Integrated Network Electronic Warfare,* formally codifying the concepts behind what would become the guiding strategy for the use of CNO during wartime.[17] He argued in a seminal article that same year that the growing importance of integrated networks, sensors, and command structures makes the destruction and protection of C4ISR systems a focal point for Chinese IW.[18]

- Both works were published with a strong endorsement from Chief of the General Staff, Gen Fu Quanyou, who lauded the groundbreaking nature of the ideas in both books; his endorsement suggests that Dai may have had powerful allies supporting this approach to IW who perhaps enabled his eventual promotion to head the General Staff Department's 4th Department, which is responsible for electronic countermeasures and it seems, the PLA's offensive CNA mission, as well.

- Dai's promotion in 2000 to lead the GSD 4th Department likely consolidated both the institutional authority for the PLA's IW mission in this organization and INEW as the PLA's official strategy for information warfare.[19]

Proponents of the INEW strategy specify that the goal is to attack only the key nodes through which enemy command and control data and logistics information passes and which are most likely to support the campaign's strategic objectives, suggesting that this strategy has influenced PLA planners toward a more qualitative and possibly effects-based approach to IW targeting. Attacks on an adversary's information systems are not meant to suppress all networks, transmissions, and sensors or to affect their physical destruction. The approach outlined by Dai and others suggests that the INEW strategy is intended to target only those nodes which the PLA's IW planners assess will most deeply affect enemy decisionmaking, operations, and morale.

- The PLA's *Science of Campaigns* notes that one role for IW is to create windows of opportunity for other forces to operate without detection or with a lowered risk of counterattack by exploiting the enemy's periods of "blindness," "deafness" or "paralysis" created by information attacks.

---

[17] OSC, CPP20020226000078, "Book Review: 'Introduction to Integrated Network-Electronic' Warfare," Beijing, *Jiefangjun Bao,* 26 February 2002.
[18] OSC, CPP20020624000214, Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," *China Military Science*, Academy of Military Science, Winter 2002
[19] Regarding the GSD 4th Department's leadership of the IW mission, see James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions Other Than Taiwan,* Roy Kamphausen, David Lai, Andrew Scobell, eds., Strategic Studies Institute, April 2009, p. 272-273.

- Dai and others stress that the opportunities created by the application of the INEW strategy should be quickly exploited with missile assaults or other firepower attacks in a combination of "hard and soft attacks" that should dominate in the early stages of a campaign.[20]

- A December 2008 article in the AMS journal, *China Military Science*, asserts that the PLA must disrupt or damage an enemy's decisionmaking capacity through a combined application of network warfare and other elements of IW to jam and control the movement of an enemy's information to achieve information superiority.[21]

Integrated Network Electronic Warfare in PLA Training

PLA field exercises featuring components of INEW provide additional insights into how planners are considering integrating this strategy across different units and disciplines in support of a campaign's objectives. IW training featuring combined CNA/CND/EW is increasingly common for all branches of the PLA and at all echelons from Military Region command down to the battalion or company and is considered a core capability for the PLA to achieve a fully informationized status by 2009, as directed by PRC President and CMC Chairman Hu Jintao.

- President Hu Jintao, during a speech at the June 2006 All-Army Military Training Conference, ordered the PLA to focus on training that features "complex electromagnetic environments," the PLA's term for operating in conditions with multiple layers of electronic warfare and network attack, according to an authoritative article in *Jiefangjun Bao.*[22]

- During a June 2004 opposed force exercise among units in the Beijing Military Region, a notional enemy "Blue Force" (which are adversary units in the PLA) used CNA to penetrate and seize control of the Red Force command network within minutes of the start of the exercise, consistent with the INEW strategy's emphasis on attacking enemy C2 information systems at the start of combat.

[20] OSC, CPP20030728000209, "Chinese Military's Senior Infowar Official Stresses Integrated Network/EW Operations," Beijing *China Military Science,* 20 April 2003. | OSC, CPP20020624000214, "Chinese Military's Senior Infowar Official Explains Four Capabilities Required," Jiefangjun Bao, 01 Jul 2003 | OSC, CPP2003728000210, "PLA Journal on Guiding Ideology of Information Operations in Joint Campaigns," 20 April 2003 | OSC, CPP2003728000210, Ke Zhansan, "Studies in Guiding Ideology of Information Operations in Joint Campaigns," *China Military Science*, Academy of Military Science, 20 April 2003.

[21] OSC, CPP20090127563002, Shi Zhihua, "Basic Understanding of Information Operation Command," *China Military Science,* 27 January, 2009.

[22] OSC, CPP20060711715001, "JFJB Commentator on Promoting PLA's Informatized Military Training" 10 July 2006.

The PLA may be using training like this to evaluate the effects of targeting enemy tactical or theater command center networks.[23]

- In October 2004, a brigade from the PLA's Second Artillery Corps, responsible for the conventional and nuclear missile forces, conducted training that featured INEW elements and relied upon a networked C2 infrastructure to maintain multi-echelon communications with a variety of supporting units and command elements while defending against EW attacks, according to PLA reporting.[24]

- A Lanzhou Military Region division, in February 2009, conducted an opposed force information warfare exercise featuring computer network attack and defense scenarios while countering electronic warfare attacks, a common feature of much informationized warfare training, according to a PLA television news program.[25]

The PLA's 2007 revised Outline for Military Training and Evaluation (OMTE) training guidance directed all services to make training under complex electromagnetic environments (CEME) the core of its campaign and tactical training, according to the director of the General Staff Department's Military Training and Arms Department.[26] ***The focus on developing capabilities to fight in informationized conditions reflects much of the core of the INEW strategy and continues to shape current and future training, suggesting that despite Dai Qingmin's retirement from the PLA, this strategy continues to serve as the core of Chinese IW***.

- The PLA has established a network of at least 12 informationized training facilities that allow field units to rotate through for exercises in environments featuring realistic multi-arms training in which jamming and interference degrade PLA communications. The flagship facility at Zhurihe in the Beijing Military Region also features the PLA's first unit permanently designated as an "informationized Blue Force," likely a Beijing Military Region armored regiment from the 38th Group Army's 6th Armored Division, according to open source reporting.[27] The blue force unit serves as a

[23] OSC, CPP20040619000083, "Highlights: Chinese PLA's Recent Military Training Activities," June 6, 2004
[24] OSC, CPM20041126000042 "Military Report" program on Beijing CCTV-7, October 31, 2004,
[25] OSC, CPM20090423017004, "Lanzhou MR Division Conducts Information Confrontation Exercise," from "Military Report" newscast, *CCTV-7, 2* February 2009.
[26] OSC, CPP20080801710005, "PRC: JFJB on Implementing New Outline of Military Training, Evaluation", 1 August 2008.
[27] Asian Studies Detachment, IIR 2 227 0141 09, "6th Armored Division, Beijing Military Region Information Systems Modernization," 26 January 2009, (U)

notional adversary employing foreign tactics and making extensive use of information technology.[28]

- The PLA's large multi-military region exercise for battalion level units, named Kuayue 2009 (Stride 2009) featured the first-ever simultaneous deployment of units from four military regions and PLA Air Force (PLAAF) units. The exercise focused on implementing the 2007 Training Outline for informationized training and included multiple mission scenarios—amphibious landing, air assault, close air support—under complex electromagnetic environments.[29]

The emphasis of the 2007 training directive on operating in complex electromagnetic environment and under informationized conditions may drive an expansion of personnel training in IW specialties—including offensive network warfare skills—to meet the demand among field units for skilled personnel. The PLA maintains a network of universities and research institutes that support information warfare related education either in specialized courses or more advanced degree granting programs. The curriculum and research interests of affiliated faculty reflect the PLA's an emphasis on computer network operations.

- The National University of Defense Technology (NUDT) in Changsha, Hunan Province is a comprehensive military university under the direct leadership of the Central Military Commission. NUDT teaches a variety of information security courses and the faculty of its College of Information Systems and Management and College of Computer Sciences are actively engaged in research on offensive network operations techniques or exploits, according to a citation search of NUDT affiliated authors.[30]

- The PLA Science and Engineering University provides advanced information warfare and networking training and also serves as a center for defense related scientific, technological, and military equipment research.[31] Recent IW-related faculty research has focused largely on rootkit design and detection,

---

[28] OSC, CPF20081205554001, "Beijing MR Base EM Training Upgrade Advances PLA Capabilities," 5 December 2008 | OSC, CPF20080912554001001, "PLA Blue Force Units Bolster Training Realism," 12 September 2008 | Dennis J. Blasko, *The Chinese Army Today,* Routledge, 2006, p. 78.
[29] OSC, CPP20090908088006," Lanzhou MR Division in 'Stride-2009' Exercise Boosts Fighting Capacity," *Jiefangjun Bao,* 7 September 2009.
[30] Profile of NUDT available at http://english.chinamil.com.cn/site2/special-reports/2007-06/26/content_858557.htm
[31] OSC, FTS19990702000961, "PRC Establishes New Military Schools Per Jiang Decree," *Xinhua,* 2 July, 1999 | "China Establishes New Military Schools," People's Daily, 7 March 1999, available at: http://english.peopledaily.com.cn/english/199907/03/enc_19990703001001_TopNews.html

including rootkit detection on China's indigenously developed Kylin operating system.

- PLA Information Engineering University provides PLA personnel in a variety of fields advanced technical degrees and training in all aspects of information systems, including information security and information warfare.[32]

Deterrence and Computer Network Operations

The Chinese government has not definitively stated what types of CNA actions it considers to be an act of war which may reflect nothing more than a desire to hold this information close to preserve strategic flexibility in a crisis. With the exception of the Taiwan independence issue, the PRC leadership generally avoids defining specific "red lines" for the use force; this is likely true for its CNA capabilities.

- Effective deterrence requires capable and credible force with clear determination to employ it if necessary and a means of communicating this intent with the potential adversary, according to the S*cience of Military Strategy*.[33]

- The *Science of Military Strategy* also stresses that deterrent measures can include fighting a small war to avoid a much larger conflict. Tools like CNA and EW, which are perceived to be "bloodless" by many PLA IW operators, may become first choice weapons for a limited strike against adversary targets to deter further escalation of a crisis.[34] This concept may also have implications for PRC leadership willingness to use IW weapons preemptively if they believe that information-based attacks don't cross an adversary's "red lines".

The PLA may also use IW to target enemy decisionmaking by attacking information systems with deceptive information to shape perceptions or beliefs. The *Science of Military Strategy* highlights this as a key contribution that IW can make in support of the overall campaign. Data manipulation or destruction may be perceived as a valuable tool to aid broader strategic psychological or deception operations or to support perception management objectives as part of a deterrence message.

- A 2003 article by the Deputy Commander of Guangzhou Military Region, entitled "Information Attack and Information Defense in Joint Campaigns,"

[32] "China Establishes New Military Schools," People's Daily, 7 March 1999, available at: http://english.peopledaily.com.cn/english/199907/03/enc_19990703001001_TopNews.html
[33] The Science of Military Strategy, p 213-215.
[34] The Science of Military Strategy, p 213-215 | OSC, CPP20000517000168, "Excerpt from "World War, The Third World War--Total Information Warfare," Xinhua Publishing House, 1 January, 2000.

published in an AMS journal, noted that information attack requires targeting both an enemy's information systems and "cognition and belief system." The primary techniques for attacking information systems, he argues, are network and electronic attack and the primary techniques for attacking people's cognition and belief system are information deception and psychological attack, which will also be implemented by CNO units.[35]

- AMS guidance on the formation of IW militia units directed that they include psychological operations elements to support perception management and deception operations against an enemy.

Some PLA advocates of CNO perceive it as a strategic deterrent comparable to nuclear weapons but possessing greater precision, leaving far fewer casualties, and possessing longer range than any weapon in the PLA's arsenal. China's development of a credible computer network attack capability is one component of a larger effort to expand and strengthen its repertoire of strategic deterrence options that includes new nuclear capable missiles, anti-satellite weapons, and laser weapons.

- Major General Li Deyi, the deputy chair of the Department of Warfare Theory and Strategic Research at the Academy of Military Sciences, noted in 2007 that information deterrence is rising to a strategic level and will achieve a level of importance second only to nuclear deterrence.[36]

- China has developed a more accurate, road mobile ICBM, the DF-31A that can range the continental United States and a submarine launched variant, the JL-2 that will eventually be deployed on China's new Jin-class nuclear powered submarine. [37]

- In 2007, China successfully tested a direct ascent ASAT weapon that used a kinetic kill vehicle to destroy an aging Chinese weather satellite[38] and in 2006, the US military accused the Chinese of using a laser dazzling weapon that temporarily blinded a reconnaissance satellite.[39]

---

[35] OSC, CPP20080314623007, "JSXS: Information Attack and Information Defense in Joint Campaigns," Beijing *Junshi Xueshu [Military Art Journal]* 1 October 2003.

[36] OSC, CPP20081028682007, Li Deyi, "A Study of the Basic Characteristics of the Modes of Thinking in Informatized Warfare," *China Military Science*, Summer 2007, p.101-105.

[37] *Annual Report to Congress: Military Power of the People's Republic of China 2006,* US Department of Defense, p. 3.

[38] *Annual Report to Congress: Military Power of the People's Republic of China 2009,* US Department of Defense, p. 14.

[39] Warren Ferster and Colin Clark, "NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft," *Space News Business Report,* 3 October 2006, available at: http://www.space.com/spacenews/archive06/chinalaser_1002.html

- Chinese researchers are working on a variety of radio frequency weapons with the potential to target satellites and other components of the US C4ISR architecture, according to US Department of Defense analysis.[40]

PLA Information Warfare Planning

An effective offensive IW capability requires the ability to assess accurately the likely impact on the adversary of a CNA strike on a given node or asset. These assessments, in turn, depend upon detailed intelligence on the adversary's network, the C2 relationships, and the various dependencies attached to specific nodes on the network.

- The *Science of Military Strategy* directs planners to "grasp the operational center of gravity and choose the targets and sequence for strike…arrange the enemy's comprehensive weaknesses on the selective basis for a list of the operational targets, according to the degree of their influences upon the whole operational system and procedure."[41]

- Mission planners must also understand the explicit and implicit network dependencies associated with a given node to avoid undesired collateral damage or the defensive redundancies that may exist to enable the targeted unit or organization to reroute its traffic and "fight through" the attack, effectively nullifying the Chinese strike.

- CNA planning also requires a nuanced understanding of the cultural or military sensitivities surrounding how a given attack will be perceived by an adversary. Failure to understand an enemy's potential "red lines" can lead to unintentional escalation of the conflict, forcing the PLA to alter its campaign objectives or fight a completely new campaign for which it may be unprepared.

PLA IW planners and leaders have noted that CNO is blurring the separation that military planners maintained between the hierarchy of "strategy," "campaign," and "combat" (or "tactics" in Western usage) so that CNO or EW weapons employed by tactical-sized units can strike strategic targets deep in the adversary's own territory beyond the range of most conventional weapons, possibly changing the course of the conflict.[42] This changing perspective on IW and especially CNO tools may impact the senior leadership perspective on targeting, particularly if the use of these tools is

[40] *Annual Report to Congress: Military Power of the People's Republic of China 2006,* US Department of Defense, p. 34.
[41] *Science of Military Strategy,* p. 464
[42] OSC, CPP20081229563002,"Relations Between Strategy, Campaigns And Battles*, China Military Science*, 29 December 2008.

perceived to have plausible deniability for Beijing or complicates an adversary's ability to counterattack.

Chinese Computer Network Operations During Conflict

Like the use of missile or air power, CNO is one of several increasingly capable warfighting components available to PLA commanders during a conflict, however, the PLA rarely discusses CNO as a standalone capability to be employed in isolation from other warfighting disciplines. Understanding how it may be used in support of a larger campaign requires Western analysts and policymakers to consider China's overall campaign objectives to understand CNO in its proper context. The current strategy for fighting a campaign in a high tech environment, reflected in the doctrinal guidance to "strike the enemy's nodes to destroy his network,"[43] directs commanders to attack the adversary's C2 and logistics networks first and exploit the resulting "blindness" with traditional firepower attacks on platforms and personnel. ***This strategy suggests that the PLA may strike with CNO and EW weapons in the opening phases of a conflict to degrade enemy information systems rather than attempt a traditional force-on-force attack directly where the PLA is at a disadvantage against more technologically advanced countries like the US.***

- Denying an adversary access to information systems critical for combat operations is influenced by principles of traditional Chinese strategic thought, but the strategy is also the result of extensive contemporary PLA analysis of likely adversaries' weak points and centers of gravity.

- While Chinese military leaders are almost certainly influenced by their strategic culture and traditions of stratagem, much of China's contemporary military history reflects a willingness to use force in situations where the PRC was clearly the weaker entity. Scholarship on the subject suggests that PRC political leaders often determined that conflict in the short term would be less costly than at a later date when strategic conditions were even less favorable to China. This logic often seems counterintuitive to the casual Western observer but reflects a nuanced assessment of changing strategic conditions and how best to align with them for a favorable outcome. PLA and PRC leaders capture this idea often when discussing the use of strategies, stratagem, or weapons that enable the weak to overcome the strong.[44]

[43] Science of Military Strategy, p. 464.
[44] There is a growing record of contemporary scholarship on strategic culture, deterrence, stratagem, and China's propensity to use force. While it is beyond the scope of the present study, a more extensive discussion of the relationship of these topics to contemporary computer network operations is essential, particularly one that moves the discussion beyond comparisons of China's military classics and toward a broader context for understanding the complexity of modern Chinese perceptions of IW and the value of CNO. For a small representative sample of some of the excellent research done on China's calculus for the use of force see: Allen S. Whiting, *China Crosses the Yalu:*

- The PLA's employment of CNO reflects an intention to use it (with EW weapons) as one element of an integrated—and increasingly joint—campaign capability. Campaign doctrine calls for using CNO as a precursor to achieve information dominance, providing "openings" or opportunities for air, naval, and ground forces to act.

CNO in any military crisis between China and the US will likely be used to mount persistent attacks against the Department of Defense's NIPRNET nodes that support logistics, and command and control functions. Attacks such as these are intended to degrade US information and support systems sufficiently for the PLA to achieve its campaign objectives before the US and its Allies can respond with sufficient force to defeat or degrade the PLA's operation. In a Taiwan scenario, for example, PLA planners likely consider the opening days as the critical window of opportunity to achieve military objectives on the island. CNO and other IW weapons that delay a US military response only increase the PLA's possibility of success without requiring direct combat with superior US forces.

- Delaying or degrading US combat operations in this Taiwan scenario sufficiently to allow the PLA to achieve lodgment on Taiwan or force the capitulation of the political leadership on the island would present the US with a *fait accompli* upon arrival in the combat operations area.

- The majority of US military logistics information systems is transmitted or accessed via the NIPRNET to facilitate communication or coordination between the hundreds of civilian and military nodes in the military's global supply chain.

Logistics Networks and Databases

In a conflict, NIPRNET-based logistics networks will likely be a high priority target for Chinese CNA and CNE. Information systems at major logistics hubs

---

The Decision to Enter the Korean War, Stanford University Press; 1960 | Allen S. Whiting, "China's Use of Force 1960-1996, and Taiwan," *International Security,* Vol. 26, No. 2 (Fall 2001), pp. 103–131 | Alastair Iain Johnston, "China's Militarized Interstate Dispute Behavior 1949-1992: A First Cut at the Data," *The China Quarterly,* 1998, No.153 (March 1998), pp. 1-30 | Alastair Iain Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*, Princeton University Press, 1998 | M. Taylor Fravel, "Regime Insecurity and International Cooperation: Explaining China's Compromises in Territorial Disputes," *International Security,* Vol. 30, No. 2 (Fall 2005), pp. 46–83 | Thomas J. Christensen, "Windows and War: Trend Analysis and Beijing's Use of Force," in *New Directions in the Study of China's Foreign Policy,* Alastair Iain Johnston and Robert Ross, eds. Stanford University Press, 2006.

either in the US Pacific Command (USPACOM) area of operations (AOR) or CONUS-based locations supporting USPACOM operations will likely be subjected to Chinese CNA and CNE operations during a conflict**.** The Chinese have identified the US military's long logistics "tail" and extended time for force build-up as strategic vulnerabilities and centers of gravity to be exploited.

- PLA assessments of US campaigns in Iraq (both Desert Storm and Operation Iraqi Freedom), the Balkans, and Afghanistan identify logistics and the force deployment times as weak points, the interruption of which will lead to supply delays or shortages. These assessments in aggregate do not seem to suggest that defeating the logistics systems will lead to a de facto US military defeat (PLA professionals likely assume that the US will implement work around and ad hoc solutions to these obstacles), but rather that these disruptions will "buy time" for the PLA as noted above.

- Logistics data of interest to PLA planners are likely areas such as specific unit deployment schedules, resupply rates and scheduled movement of materiel, unit readiness assessments, lift availability and scheduling, maritime prepositioning plans, air tasking orders for aerial refueling operations, and the logistics status of bases in the Western Pacific theater.

- *US Joint Publication 4-0: Joint Logistics* notes that "the global dispersion of the joint force and the rapidity with which threats arise have made real-time or near real-time information critical to support military operations. Joint logistic planning, execution, and control depend on continuous access to make effective decisions. Protected access to networks is imperative to sustain joint force readiness and allow rapid and precise response to meet JFC requirements."[45]

- Potential Chinese familiarity with the network topology associated with US Transportation Command (USTRANSCOM) or related logistics units on NIPRNET could aid CNE missions intended to access and exfiltrate data related to the time-phased force and deployment data (TPFDD) of a specific contingency or operations plan. A TPFDD is the logistics "blueprint" for the sequence of movement of supplies and is based on a commander's expression of priorities for personnel and materiel to move into a combat theater.

The Chinese may attempt to target potentially vulnerable networks associated with strategic civilian ports, shipping terminals, or railheads that are

[45] *US Joint Publication 4-0: Joint Logistics,* 18 July 2008, US Department of Defense, p.I-5 available at: http://www.dtic.mil/doctrine/jel/new_pubs/jp4_0.pdf

supporting the military's movement of critical supplies and personnel. Maintaining effective movement control during a major mobilization is inherently complex. Disruptions of information systems at key nodes, particularly "downstream" at shipping terminals or airports, while not catastrophic, could create major delays as the traffic en route to the affected destination is forced to slow or halt, similar to the cascading traffic delays that can result from a minor accident at rush hour.

- *US Joint Publication 4-0: Joint Logistics* also points out that "inventory management capitalizes on authoritative information (accurate, real-time, and widely visible) and performance trends to inform decisions about attributes of the materiel inventory throughout the supply chain. Maintaining optimal stockage levels and accountability of materiel throughout the supply chain enables the joint logistician to manage the flow of materiel between strategic and tactical supply nodes to meet warfighter requirements." [46]

- Many logistics databases on NIPRNET have Web-based interfaces to enable ease of access, but may only require PLA operators to compromise one weak password via keystroke logging or to exploit SQL injection vulnerabilities on the Website to gain user-like access.

- Long term access to NIPRNET via CNE techniques—and to logistics information supporting the TPFDD for various warplans in particular—also allows the PLA to assemble a detailed current intelligence picture of the intended US force deployment packages for specific contingencies.

The PLA's basic CNE/CNA strategy against NIPRNET logistics databases is likely a combination of attacks on selected network segments to limit both the flow and possibly corrupt the content of unencrypted data. An attack on logistics information systems may begin by exploiting previously compromised hosts on the network held as a kind of war reserve in the event of a crisis.[47]

- If PLA operators target a unit or network segment that does not authenticate HTTP traffic (common Internet traffic) through a proxy server before leaving the network, they will be able to operate much more freely on the network. An attacker in this environment can connect out to a remote C2 node and download additional tools or exfiltrate (and infiltrate) data without a requirement for valid user credentials.

[46] *US Joint Publication 4-0: Joint Logistics,* p. JP-40
[47] The attack techniques may shift as changes to US INFOCON levels limits accessibility of some applications or external connections and prioritization on network traffic affects the types of inbound traffic permitted through firewalls.

Reporting of attacks on US networks attributed to China suggests that these operators possess the targeting competence to identify specific users in a unit or organization based on job function or presumed access to information. Access that exploits legitimate user credentials can allow the attacker to review file directories and potentially target specific files for exfiltration or alteration, depending on the mission requirements and the US INFOCON levels. Alternately, these operators can use this access for passive monitoring of network traffic for intelligence collection purposes. Instrumenting these machines in peacetime may enable attackers to prepare a reserve of compromised machines that can be used during a crisis.

- Chinese CNO operators likely possess the technical sophistication to craft and upload rootkit and covert remote access software, creating deep persistent access to the compromised host and making detection extremely difficult.

- An "upstream" attack on the networks of civilian contractors providing logistics support to operational units also has potential for great impact and is potentially easier against smaller companies that often lack the resources or expertise for sophisticated network security and monitoring.

- Many of the vulnerabilities outlined above can be greatly minimized if the network uses a proxy server, implements firewall blocks of unproxied access, blocks proxy access without valid user authentication, and prevents user credentials from being exposed to the attackers.

Chinese CNO operators may also attempt to attack US perceptions of the validity of data in these networks by uploading false records or corrupting existing records, possibly for intentional detection. This discovery may generate a manpower and resource intensive review of the targeted unit's database records or other files against a known good back up copy before the unit resumes normal operations, creating potentially costly operational delays. If this type of attack is staged against several large or critical supply nodes, the impact could be significant.

- Uploading files or accessing existing records in NIPRNET-based logistics databases would require PLA operators to compromise a computer on the targeted LAN and be able to operate with the local users' credentials, a capability observed in past intrusions of US networks that are attributed to China.

- The discovery of this type of attack may have a greater impact on US forces from a perception management or psychological operations perspective than the more localized targeting to redirect supplies.

- Only a limited number of actual compromises may be required to have a disproportionate impact on US operational tempo if information security concerns require time consuming validation of logistics or other databases by systems administrators and logistics personnel across the theater or in CONUS.

Command and Control Data

Much of the operational traffic between command entities and subordinate units such as unit location, status, situation reports, and deployment orders, is transmitted via classified systems both in peacetime and wartime. Conducting CNO to penetrate and compromise the encryption and defensive layers built into the architecture of these systems is a resource intensive and time consuming process for Chinese IW units or the civilian researchers likely supporting them. ***The Chinese doctrinal orientation toward attacking an enemy's information flow suggests that if a classified network is attacked, it will likely be intended to impede encrypted traffic flow if it moves across an unclassified backbone rather than attempting to decrypt data or penetrate into the actual network.***

- Even if a sensitive encrypted network is not compromised, focused traffic analysis of encrypted communications via computer network exploitation may still yield useful information.

- If PLA CNO operators are tasked with targeting the networks or databases of specific US military units, then basic network reconnaissance conducted during peacetime can support offensive operations during wartime.

- Once these units or databases are identified, an attacker can use common techniques or tools to affect a denial of service attack against any server or router. The sophistication of this type of attack is within the assessed technical capabilities of many individuals in China's hacker community and likely of PLA units with trained CNO operators.

- Some CNE operations may be designed for purely reconnaissance purposes to map out network topologies and understand the command and control relationships of specific areas of US military or commercial networks rather than exfiltrate data or emplace "sleeper" malicious software on targeted machines.

PLA CNO commanders and operators likely recognize that a capability for peacetime compromise is not a guarantee of wartime access. US INFOCON levels will increase during a crisis, blocking access to some or all of an adversary's pre-instrumented

machines. Ongoing probes and compromises designed to elicit changes in US defensive posture may, however, provide some insights into how the network environment will change during periods of heightened threat. Chinese operations, therefore, could also include efforts designed to create intentional "noise" on the network that elicits a reaction, allowing the attackers to gather intelligence on how the US defensive posture will change under select circumstances. This is a cyber parallel to US Cold War-era electronic warfare operations that were designed to provoke a reaction from Soviet air defense networks to collect intelligence on their responses to various types of threats.

Key Entities in Chinese Computer Network Operations

General Staff Department Fourth Department

The GSD 4th Department's traditional offensive EW mission, Dai Qingmin's leadership of the department during the first half of this decade, and open source reporting that references the Department's role in implementing INEW, all suggest that it has the primary authority for offensive IW in the PLA.

- The 4th Department, also referred to as the Electronic Countermeasures Department (ECM) Department, oversees both operational ECM units and R&D institutes conducting research on a variety of offensive IW technologies.

- The 4th Department's oversight of IW dates to at least 1999 and probably earlier. Recent scholarship notes that Dai Qingmin's seminal work, *On Information Warfare,* was vetted by the 4th Department prior to its publication in 1999 indicating that it had organizational oversight of this topic even at that time.[48]

- The GSD's decision in 2000 to promote Dai Qingmin to head the 4th Department—vetting his advocacy of the INEW strategy—likely further consolidated the organizational authority for the IW—and the CNA mission specifically—in this group. Dai's promotion to this position suggests that the GSD probably endorsed his vision of adopting INEW as the PLA's IW strategy.

General Staff Department Third Department

The GSD Third Department's longstanding signals intelligence (SIGINT) focus, historical lack of an offensive role, and its large staff of trained linguists and technicians makes it well suited for oversight of the CND and CNE missions in the PLA. The 3rd Department maintains an extensive system of signals collection stations throughout China with collection and processing stations co-located with each of the PLA's Military Region headquarters.[49] It is tasked with the foreign signals collection, exploitation, and analysis and also communications security for the PLA's voice and data networks. This latter responsibility may encompass network defense

[48] Mulvenon, PLA Computer Network Operations, p. 272. | See also OSC, FTS20000105000705, "Fu Quanyou Commends New Army Book on IW," *Jiefangjun Bao*, 7 December 1999.
[49] Desmond Ball, "Signals Intelligence In China" *Jane's Intelligence Review,* 1 August, 1995.

as well, though little information is available to confirm this role.[50] Some Western analyses of the 3rd Department claim it maintains a staff of more than 130,000, though this figure cannot be independently confirmed. Regardless of the specific figure, accessibility to a large staff of highly skilled linguists and technical analysts would provide significant depth for a computer-based intelligence collection and exploitation mission.

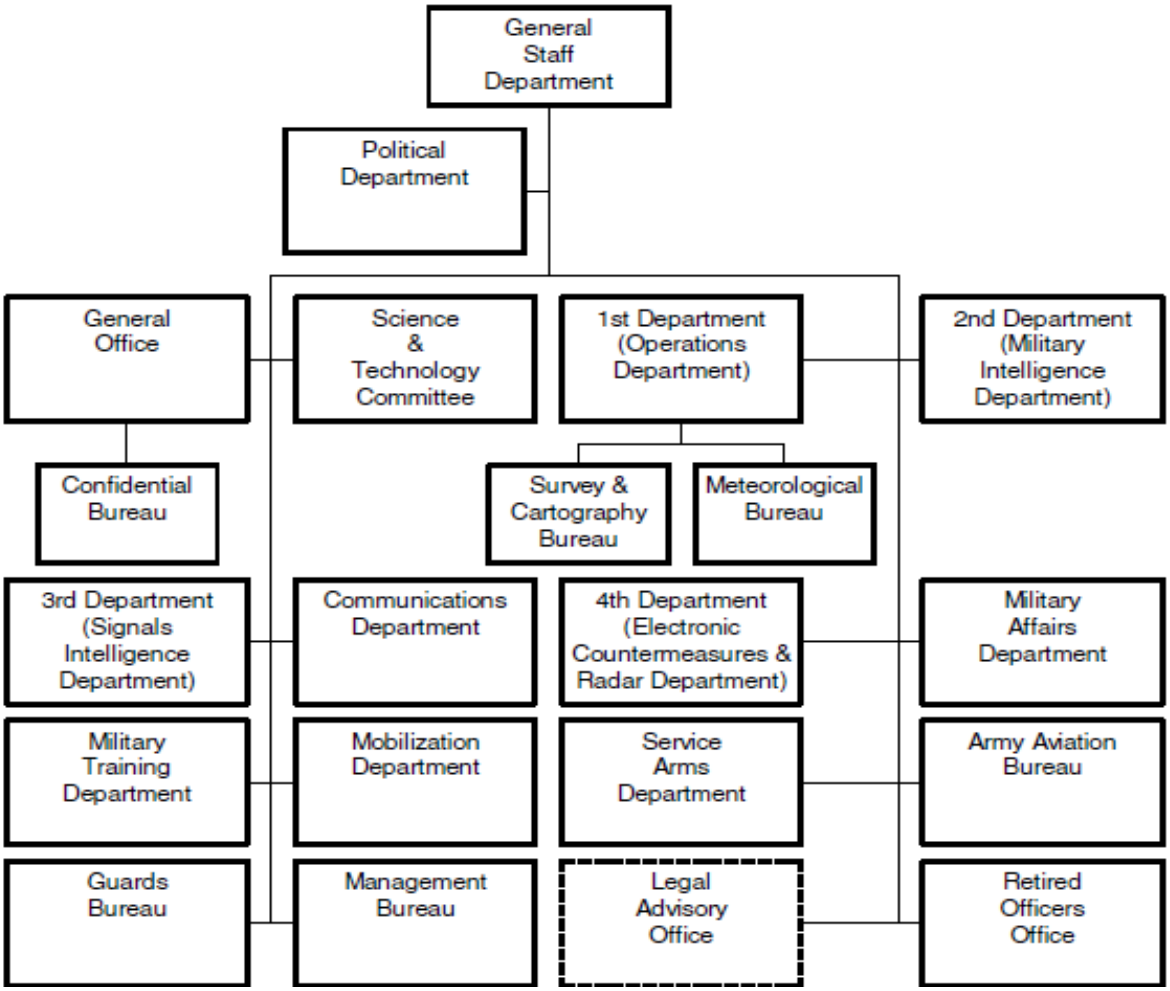


Figure 1: General Staff Department of the People's Liberation Army[51]

[50] OSC, CPP20060110510011, "HK Journal Details History, Structure, Functions of PRC Intelligence Agencies," Hong Kong *Chien Shao,* No 179, 1 January 2006. | Mark A. Stokes, *China's Strategic Modernization: Implications for the United States*, U.S. Army Strategic Studies Institute, September 1999, p. 34.

[51] Organizational chart from "The General Staff Department Of The Chinese People's Liberation Army: Organization, Roles, & Missions," by David Finkelstein, in *The People's Liberation Army as Organization Reference Volume v1.0*, James C. Mulvenon and Andrew N. D. Yang, eds, RAND Corp., 2002.

Technical Reconnaissance Bureaus

The PLA maintains at least six technical reconnaissance bureaus (TRB) located in the Lanzhou, Jinan, Chengdu, Guangzhou, and Beijing military regions that are responsible for SIGINT collection against tactical and strategic targets and have apparent CNO duties, though few details are available on the exact role or subordination of these units.[52] The TRB's probable subordination under the 3rd Department suggests that their CNO responsibilities are likely focused on defense or exploitation of foreign networks. While the TRB appear largely focused on traditional SIGINT missions, oblique references to staff from these units conducting advanced research on information security or possibly related topics suggests a possible CNO or EW role that augments their SIGINT collection mission.[53]

- TRB affiliated staff have also performed information assurance certification for other PLA units, according to reporting from a Party affiliated newspaper.[54]

- In 2002, the Third TRB, described as a "technical rapid reaction unit," received its fifth consecutive award for outstanding "research in information warfare theories," and the development of new technical means of operation, according to a local Party affiliated media outlet. These dates and numbers suggest that as early 1997, this TRB possibly began including IW in its mission.[55]

- The First TRB in Chengdu received a series of military commendations for "substantial achievements in informatization building," academic research

---

[52] Dennis Blasko, "PLA Ground Force Modernization and Mission Diversification: Underway in all Military Regions," in *Right Sizing the People's Liberation Army: Exploring the Contours of China's Military,* Roy Kamphausen, Andrew Scobell, eds., Strategic Studies Institute, September 2007, p. 366-372 | Ellis L. Melvin, *A Study Of The Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureau*, June 19, 2005 | Virtual Information Center, People's Republic of China Primer, 04 August 2006, available at: http://www1.apan-info.net/Portals/45/VIC_Products/2006/08/060804-P-China.doc.

53 OSC, CPP20071011318004, "Chengdu MR Unit 78006 Praised for Breakthroughs in 'Cutting-Edge' IT Research," *Chengdu Zhanqi Bao*, 20 August 2007 | OSC, CPP20070122478002, "Shenyang MR Unit 65016 Members: Information Warfare is not Informationized War," 22 January 2007.

[54]OSC, CPP20081211478016, "PLA Unit 65016 Network Security Team Conducts 'Blanket' Security Check," Shenyang *Qianjin Bao* 18 October 2008, p. 1.

[55] OSC, CPP20030411000212, "Roundup of C4I Activities in PRC: 5 Nov 2002-12 Mar 2003," 5 November 2002" | Ellis L. Melvin, Ibid.

awards, and a computer network defense project that was vetted for use by a GSD level technical appraisal, according to PLA reporting.[56]

PLA Information Warfare Militia Units

Since approximately 2002, the PLA has been creating IW militia units[57] ***comprised of personnel from the commercial IT sector and academia, and represents an operational nexus between PLA CNO operations and Chinese civilian information security (infosec) professionals.***[58] The PLA has established militia units directly within commercial firms throughout China to take advantage of access to staff with advanced education, modern commercial-grade infrastructure, sophisticated software design capabilities, and the greater likelihood of finding "politically reliable" operators.[59]

- A political commissar for the Guangzhou People's Armed Police (PAP) garrison advocated in 2003 the direct involvement of urban militia units in information warfare, electronic warfare, and psychological warfare; He also proposed that militia reform efforts should focus on making information warfare one of the Guangzhou militia's primary missions.[60]

- A Tianjin-based militia garrison restructured subordinate units in 2004 to increase capabilities for operations under informationized conditions, including the creation of a dedicated information operations unit, according to the PLA Daily.[61]

---

[56] OSC, CPP20081113563001, "China: PLA Activities Report 1-15 Oct 08," 13 November 2008

[57] The PLA's 8 million strong militia system, under the control of the State Council and the Central Military Commission (CMC), is an active reserve system comprised of males 18-35 who are not currently serving in the PLA; the militia system augments active duty PLA units in virtually every area of military operations. See: *China's National Defense in 2004*, Information Office of China's State Council, December 2004, http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html | *China's National Defense in 2006*¸ Information Office of the State Council of the People's Republic of China, December 2006, Beijing, available at: http://english.chinamil.com.cn/site2/news-channels/2006-12/29/content_691844.htm

[58] OSC, CPP20031002000138, "Telecom Experts in Guangzhou Doubling As Militia Information Warfare Elements," *Guofang,* Academy of Military Science, 15 September 2003 | OSC, "PLA C4ISR Activities Roundup, 1 April-30 May 2006.

[59] OSC, CPP20031002000138, Ibid.

[60] Lu Qiang, "Focus On The Characteristics Of Information Warfare To Strengthen The City Militia Construction" *China Militia Magaz*ine, August 2003, available at: http://www.chinamil.com.cn/item/zgmb/200308/txt/16.htm

[61] OSC, CPP20050301000186, "Roundup of C4I Activities in PRC, 13 November 2004-15 January 2005," 15 January 2005.

- A Henan province military sub-district in 2007 organized militia units for communications and network warfare; starting in 2008, an Anhui Province unit recruited militia personnel from large private enterprises for specialized technical training, according to PLA media sources.[62]

Figure 2: The Yongning District Information Operations Militia Unit office, Lanzhou Military Region.

Figure 3: Meeting to Establish the Yongning County IW Militia.

PLA media reporting indicates that IW militia units are tasked with offensive and defensive CNO and EW responsibilities, psychological warfare, and deception operations, though the available sources do not explain the lines of authority, subordination, or the nature of their specific tasking.[63]

- A militia battalion in Yongning County (Ningxia Province, Lanzhou Military Region) established an IW militia group in March 2008 and tasked it to conduct network warfare research and training, and to "attack the enemy's wartime networks" according to the unit's Website. [64]

[62] OSC, CPP20080601711001, "Table of Contents Report: China Militia (Zhongguo Minbing)", 10 March 2008. | OSC, CPP20080615711001, "Table of Contents Report: China Militia" 10 April 2008.

[63] "*Minbing Wangluo Zhan Fendui Zhize* (Duties of the Network Warfare Militia Unit), 16 March, 2008, available at: http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp?infoNo=26366. | China And Northeast Asia," *Jane's Sentinel Security Assessment* , April 3, 2009. | OSC CPP20090102670001, "PRC S&T: Ezhou Militia Establishes Network Presence," *Guofang,* Academy of Military Science, May 2001. | OSC, CPP20031002000138 "Telecom Experts in Guangzhou Doubling As Militia Information Warfare Elements," *Guofang,* Academy of Military Science, 15 September 2003.

[64] "Yongning is the First to Set Up Information Warfare Militia Units," 19 March, 2008, available at: http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp

- The Yongning unit is composed of an information warfare center detachment (*xinxi fendui zuozhan zhongxin*), information gathering detachment (*minbing xinxi souji fendui*), militia network warfare unit (*minbing wangluo zhan fendui*), and a militia network protection unit (*minbing wangluo fanghu fendui*), suggesting that this unit is responsible for the full range of CNO missions.[65]

In early 2003, AMS published an account of a probable proof of concept initiative in the Guangzhou Military Region to establish IW militia units using local telecommunications companies as a base from which to draw personnel, financial support, and infrastructure access, suggesting that the PLA was tapping its growing pool of civilian commercial IT expertise to aid military information warfare requirements. The Guangzhou Garrison created four "Militia Information Technology Battalions" in local firms comprised of CNO and offensive and defensive EW units.[66]

- The officers conducted a detailed census of Guangdong's Dongshan District, where the IT sector is concentrated, to identify people with specific backgrounds, such as advanced degree holders, people who had studied overseas, people credited with major scientific research achievements, and computer networking experts, suggesting that this unit is tasked with more sophisticated network operations that require both advanced technical expertise and knowledge of foreign languages or cultures.[67]

- The battalion included a headquarters unit, a computer network operations company with attack and defense platoons, and an EW company with electronic reconnaissance and deception platoons.

- No unit level training materials existed prior this, according the officers responsible for creating this unit, forcing them to draft a "Training Plan for Militia Information Technology Elements," with input from Guangzhou military region headquarters units and an unspecified "electronic countermeasures regiment," a likely reference to a GSD 4th Department subordinate unit. This lack of training materials suggests that it may have been one of the earliest such units, possibly a proof of concept that the AMS was vetting.

---

[65] *Minbing Wangluo Zhan Fendui Zhize* (Duties of the Network Warfare Militia Unit), 16 March, 2008, available at: http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp?infoNo=26366.
[66] OSC, CPP20031002000138, Ibid. The exact date of creation for this unit is not specified in this article, published in late 2003, however, the authors make reference to a series of these units' technical accomplishments that suggest the battalions were operational at the time of writing.
[67] OSC, CPP20031002000138, Ibid.

Research responsibilities for this battalion included operational methods for "launching hacker attacks, propagating viruses, jamming information channels, and disrupting nodes of enemy networks" indicate that this particular unit was responsible for offensive R&D in addition to operational CNE duties.[68]

Within three years of the Guangzhou unit's creation, the AMS published a second article on the concept that explicitly endorsed the formation of IW militia and directed the PLA to make the creation of these units a priority.[69] The model presented followed closely what the Guangzhou Garrison created three years earlier, suggesting the idea was now fully vetted and had a senior leadership mandate.

- The AMS authors directed garrison level commands to establish these units with personnel from local commercial IT industries and universities and train them in simulated network warfare environments to develop their skills in all aspects of IW and to create a mix of specialized units skilled in electronic warfare, network warfare, and psychological warfare.[70]

- Garrison commanders were also instructed to relax the militia's standard age and physical fitness requirements, likely to ensure that individuals with highly valued technical skills are not eliminated unnecessarily.

Authoritative PLA writings on these units display a clear sensitivity to the potential diplomatic impact resulting from the exposure of these units' targeting of foreign networks or the potential proliferation of their tools outside the units' control. Possibly as a result of this sensitivity, the AMS authors recommend unusually strict security precautions for militia units—particularly in vetting and monitoring personnel—likely a reflection of their highly sensitive work.

- The 2006 AMS article notes that many countries view network reconnaissance, electronic jamming, and "network invasion" as serious issues that may even be considered acts of war, one of the few such explicit acknowledgements by the PLA.

- Garrison commanders are urged to ensure that "individual behavior is monitored and work results do not proliferate," a possible reference to guarding against leaks of classified information or software tools developed by unit members.

[68] OSC, CPP20031002000138, Ibid.

[69] OSC, "PLA C4ISR Activities Roundup, 1 April-30 May 2006.

[70] OSC, "PLA C4ISR Activities Roundup, 1 April-30 May 2006."

- Open source reporting on these units is limited to descriptions of their creation and general organization. Research did not uncover materials outlining details of their peacetime operations. These units may be focused on supporting purely military operational requirements such as gathering intelligence on foreign military networks to support contingency planning for CNA missions.

Regardless of the specifics of the mission, the PLA is clearly turning to its civilian IT workforce as this resource base continues to grow. While traditional hackers offer unique skill sets in some cases and may have a niche role for PLA or state intelligence collection, the PLA clearly is looking to its increasingly mature base of civilian IT expertise to round out its IW ranks.

The Chinese Hacker Community

China's hackers, active in thousands of Web-based groups and individually, represent a mature community of practitioners that has developed a rich knowledge base similar to their counterparts in countries around the world. A review of these Web communities reveals many layers of interest groups: malware tool developers, legitimate security researchers, and novices and experts alike in search of training. The tools or techniques that these groups post are often used by true black hat practitioners.

China's hacker community gained early notoriety for member willingness to engage in large-scale politically motivated denial of service attacks, data destruction, and Web defacements of foreign networks, known as hacktivism. Between 1999 and 2004, the Chinese hacker community was defined by its regular use of large scale, politically motivated attacks against foreign networks or Websites. Chinese hackers traded Web defacements and distributed denial of service attacks with their counterparts in the United States, Japan, Taiwan, Indonesia, and South Korea and operated with relative immunity from Chinese law until strongly worded condemnations issued from Beijing eventually reigned in the attacks. Motivated by nationalist fervor, often resulting from a perceived insult to China by a foreign country, the leaders of hacker groups unified their members, identified targets, and often disseminated attack tools via their Websites to ensure mass participation.

- In May 1998, anti-Chinese riots in Indonesia sparked a series of Chinese hacker attacks on multiple Indonesian Websites.

- Following the accidental bombing of the PRC embassy in Serbia in May 1999, Chinese hackers mounted their first large scale attack on the White House led by the group Javaphile according to one of its founding members, who uses the "screen name" *CoolSwallow*.[71]

[71] Scott Henderson, *The Dark Visitor,* January 2007, p. 36.

- The 1999 comments by then Taiwan President Lee Teng-hui that Taiwan deserved to be treated as an equal state by the PRC catalyzed massive PRC hacker attacks on the Taiwan National Assembly, Presidential Executive Office and many additional government Websites, according to Western press reports of the exchange.[72]

- In May 2001, the Honker Union of China claimed that it had attacked over 1,000 US Websites—approximately the same number that US hackers claimed they attacked in the PRC—following the collision between a US EP-3 surveillance aircraft and a Chinese fighter.[73]

PRC government reaction to Chinese hacker group participation in the various "hacker wars" from 1999 to 2002 was initially encouraging, lauding the efforts of the various Chinese groups involved. By mid 2002 and after, however, this sentiment changed and official Party media sources published editorials discouraging further mass actions online, suggesting that hacking activities in any country were illegal and would not be tolerated.[74] The groups interpreted the editorial as state opposition to future planned attacks and gradually stood down.

- In 2001, following a large scale denial of service attack against the White House, the People's Daily, the official newspaper of the Communist Party, issued an editorial in its online edition that decried the Chinese attacks as "Web terrorism," and said that the attacks by the Honker Union of China on US Websites were "unforgivable acts violating the law," effectively withdrawing Beijing's tacit and explicit support from the hacker groups' campaigns.[75]

- As government tolerance for large scale attacks against foreign networks waned, many of the most prominent Chinese hacker organizations active in the US-China and cross-Strait exchanges at the beginning of the decade appear to have evolved into formal information security research companies offering professional information security services. Many others simply disbanded, or reorganized. Some of these groups or individuals have developed relationships with companies close to PRC security organizations or to the government itself.

---

[72] Damon Bristow, "Cyber-warfare rages across Taiwan Strait," *Jane's Intelligence Review,* Vol. 12, Issue 2, February 1, 2000.
[73] OSC, CPP20010510000031, "Chinese Hackers Call for Ceasefire in Sino-US Hacker War," *AFP*, 10 May 2001.
[74] OSC, CPP20010508000067, "SCMP Report on PRC Officials Condemning Hacker Attacks," by Vivien Pik-kwan Chan, *South China Morning Post*, 8 May 2001.
[75] OSC, CPP20010508000067, Ibid.

The government's position on these activities created a dynamic of self-censorship,[76] and effectively deterred a general resurgence of similar large scale hacker wars. Some groups, rallying around politically "safe" topics such as anti-Tibetan independence, however, still attempt politically driven attacks on foreign Websites.

- In December 2008, Chinese hackers associated with the Web group hack4.com staged politically motivated Web defacements on French Embassies in the US, United Kingdom, China, and Canada after French President Sarkozy's December 2008 visit with the Dalai Lama.

- Chinese hackers attempted unsuccessfully to stage a large scale distributed denial of service (DDoS) attack against CNN's Website in April 2008, with purpose-built malware that ordinary Internet users could employ in a crude but potentially effective attack. The planning for the attack was exposed by a US-based information warfare expert on his blog and the volume of traffic against CNN generated from this effort barely registered among Internet security analysts as a denial of service attack.[77]

A February 2009 National People's Congress expansion of China's anti-hacking law, coupled with a series of high profile arrests and harsh sentences for hacking crimes, will possibly subject China's online hacker communities to greater scrutiny and possibly discourage some of the overt exchange of tools and hacking advice in open online forums.

- Previously China's anti-hacking law only prohibited intrusions into PRC government computer systems, technically leaving China's hackers extremely wide latitude for cybercriminal activities. The amendment also added a section criminalizing the creation and dissemination of malicious software.[78]

- Security authorities have already used the law for several high profile arrests and convictions of both amateur and well-established hackers.

---

[76] Mulvenon, "PLA Computer Network Operations," p. 279.
[77] See Scott Henderson's *Dark Visitor* blog at http://www.thedarkvisitor.com/2008/04/new-kinda-lazy-chinese-hacker-attack-on-cnn-scheduled-for-tomorrow/; and security researcher Jose Nazario's blog at Arbor Networks, at http://asert.arbornetworks.com/2008/04/cnn-attacks-inside-two-dedicated-ddos-tools/; Mr. Henderson first detected the discussion threads on the attack planning and notified CNN. Both he and Mr. Nazario maintained an ongoing watch on the developments via their respective blog sites, publicizing the plans while attempting to update CNN system administrators.
[78] "China Toughens Cybercrime Rules," *Computerworld*, May 19, 2009, available at: www.computerworld.com/china_toughens_cybercrime_rules. | "Chinese Lawmakers Consider Tough Penalties on Hackers," *Xinhua*, December 22, 2008, available at: http://news.xinhuanet.com/english/2008-12/22/content_10544179.htm. | OSC CPP20090404718012, "Law Revision Tars "Patriotic" Hackers With Same Brush as Thieves And Troublemakers," *South China Morning Post Online,* 4 April 2009.

Hacktivist Support to the State

Little in the internal writings on Chinese INEW strategy or other writings on IW theory or strategy suggests that the PLA or state security bureaus intend to use hacktivist attacks as a component of a CNO campaign and there is little compatibility between the principles of the INEW strategy as they are known from open sources and the common characteristics of most hacktivist attacks. While the simple absence of PLA discussions of the topic—or the absence of sources in which it is discussed—does not prove an unwillingness to engage hacker groups in these types of attacks, several factors argue against formal PLA plans to include hacktivism as part of a CNO campaign in wartime.

- *Command and Control*: The lack of an easily implemented command and control structure from the PLA to the hacker community at large makes guiding or directing attacks extremely difficult. Once initiated, hacktivist attacks have the potential develop their own momentum and begin operating beyond the PLA's or civilian government's ability to easily control the participants or their targeting. Self-generating hacktivist attacks also have the potential to interfere with sensitive CNO missions by inadvertently disrupting the PLA's own computer network attacks. Hacktivist attacks on a Chinese adversary may also risk shutting down lines of communication in use for intelligence collection or accidently overwhelm channels the PLA is using as feedback loops to monitor the effectiveness of their network attacks.

- *Precision Targeting*: The core principles that seem to guide the INEW strategy are based on precision targeting and disciplined coordination to strike carefully selected nodes of an enemy's information systems judged to have maximum operational impact. The goal is to establish control over the adversary's ability to access or disseminate information. Hacktivist target selection, in contrast, is generally based on political or nationalist symbolism and not on an alignment with real or perceived PLA campaign objectives and may actually hinder PLA operations or intelligence gathering. Chinese hackers reportedly destroyed large volumes of data on the US Web servers they attacked during the US EP-3 crisis in April 2001.[79] Similar data destruction against US military servers during a conflict may eliminate valuable intelligence sources for the PLA or destroy data already altered by the PLA as part of a larger deception or perception management operation. Large scale distributed denial of service attacks or high profile Web defacements can also potentially undo

[79] OSC, CPP20010510000031, "Chinese Hackers Call for Ceasefire in Sino-US Hacker War," *Agence France Presse,* 10 May 2001.

backchannel or even overt diplomatic efforts to resolve a crisis or negate the effects of carefully crafted psychological operations.

- *Indications and warning*: Surprise and deception are central to the INEW strategy and Chinese hacktivist attacks generally lack both. Online mass organization is inherently public and while many hacker groups may implement nominal vetting of members or attempt to close their discussion threads, there is still a need to publicize the cause, announce the targets and if necessary, disseminate tools; all of which greatly increases the likelihood that the plans will be detected and successfully countered. The organizers of the attempted CNN DDoS attack rescheduled their attack and changed Websites in part because of publicity generated by the US-based researchers noted previously who monitored the attack preparations on the Chinese hacker Websites and alerted CNN.

Hacker-State Collaboration

While the PRC government appears reluctant to use hacktivism as a CNO tool, there may be a willingness to establish direct relationships with highly skilled individuals or small groups in the hacker community. The PRC government may also be able to engage commercial firms comprised of experienced hackers and operating as nominally legitimate information security groups***.*** This engagement ranges from simple job recruitment by government security ministries on hacker Websites to possible support from blackhat code developers for organized intrusions into US Government and commercial networks.

Commercially-based white hat information security researchers (i.e. those pursuing overt legal research in the field) are developing extensive government customer bases for hardware and possibly software support. Many of the most prominent groups from earlier in the decade and their leaders have either disbanded or transformed themselves into seemingly legitimate security firms. Large groups like Xfocus and Black Eagle Base have reshaped themselves into commercial operations, albeit in close alignment with state security and information security objectives.

- NSFocus, a prominent commercial information security firm, evolved out of the Green Army Alliance, an early—and prominent—hacker group active from 1997 through 2000; the NSFocus Website still retains logos of the Green Army Alliance and the list of its founding members features some of the most prominent hackers in China.[80]

[80] Scott Henderson, *The Dark Visitor,* p.29

- XFocus, a commercial information security company that grew from a hacker group, annually co-sponsors XCon, one of the largest "hacker conferences" in China in partnership with NSFocus and Venus Technology.

- Henan Provincial Public Security Bureau authorities shutdown The Patriot Hackers-Black Eagle Base Website and arrested its members in February 2006. The group, however, was operational again six months later under the name Black Eagle Honker Base when its members released a statement claiming that the group vowed to focus its efforts on training people for the state and working to improve the state's network security industry, suggesting a possible cooperative relationship with state authorities as a condition of their release.[81]

- The Black Eagle leadership also expressed appreciation to the State Security Bureau (*guojia anquan ju)* and the Commission of Science and Technology in National Defense (COSTIND, and now renamed SASTIND[82]) for the educational guidance they provided to members while in custody. The latter, entity, charged with overseeing national defense industry policy, is not typically referenced in connection with hacker groups or their activities.[83]

Individuals, or possibly groups, engaged in computer network exploitation against US networks have obtained malicious software developed by Chinese underground or black hat programmers. The ability to obtain this custom code indicates that these operators have ties to select members of the hacker underground.

In one demonstrated instance, black hat programmers affiliated with Chinese hacker forums provided malicious software to intruders targeting a US commercial firm in early 2009. The techniques and tools employed by this group or individual are similar to those observed in previous penetration attempts against this same company in the previous year, according to their forensic analysis.

- Forensic analysis also suggests this group is comprised of multiple members of varying skill levels, operating with fixed schedules and standard operating procedures and is willing to take detailed steps to mask their activities on the targeted computer.

[81] OSC, CPP20060810443001, "Patriot Hacker Website 'Restored' After 'Guidance," 10 August 2006
[82] In March 2008, the Commission on Science and Technology for National Defense (COSTIND) was reorganized and subordinated to the Ministry of Information Industry and Technology (MIIT) and is now called State Administration on Science and Technology for National Defense (SASTIND).
[83] OSC, FEA20060811026153, "PRC Patriot Hacker Website Restored After Guidance," 10 August 2006.

- Open source research on the screen name of the coder who created the malware used in the early 2009 attack revealed that the individual is likely a native Chinese speaker who posted a keystroke logging program with rootkit elements to a discussion board on a prominent Chinese hacker group Website known as EvilOctal.

- The coder created the PDF document used as the attachment to carry the malicious software with a tool that is only available in Chinese called FreePic2Pdf, version 1.26; this document was modified to covertly install a zero day exploit that targeted a previously unknown vulnerability in Adobe Acrobat.[84]

- Upon successful installation on the victim system after the user opened the attachment, the Trojan horse malware began periodically attempting to connect with another machine overseas, essentially sending a beacon to let the attackers know that a machine had been successfully attacked. The intruders only completed this connection when they were ready to commence the next phase of the operation via encrypted communications with the victim computer.

- The operators worked in a three shift, 24 hour cycle issuing reconnaissance commands identical to those observed in previous attacks.

- When significant differences were recognized between this computer and previously compromised systems on the same network, the attack team extracted small amounts of data to determine the configuration of security software installed and their ability to access targeted data on the company's network.

- The operators installed a rootkit, which gives the attacker privileged access to a victim computer while remaining undetectable, suggesting the attackers intended long-term covert use of the victim computer. The attackers configured the rootkit to execute upon the next system reboot, effectively hiding the operators' files, programs, network connections and registry settings, however, operator error caused a problem in the rootkit execution and locked the attackers out of the targeted computer, ending the operation, according to forensic analysis.

[84] See details on this vulnerability at: http://www.adobe.com/support/security/advisories/apsa09-01.html and http://www.kb.cert.org/vuls/id/905281.

- The rootkit code is still not publicly available, suggesting that the attacker obtained it directly from the coder or someone with direct access to this individual.

The creator of another zero day exploit used to target US companies in the fall of 2008 developed the code in Chinese and on a machine with Chinese set as the default language indicating that this individual was also likely a native or fluent speaker. Little additional detail about the developer's identity is available from forensic analysis but it reinforces the assertion that a relationship exists between Chinese black hat programmers and individuals responsible for intrusions into US networks.

- US companies began receiving small waves of spam-like emails with a Microsoft WordPad (.wri) file attachment containing a small piece of malicious software that acted as a Trojan, enabling the attackers to gain complete access to the targeted computers, a hallmark of the computer network exploitation tradecraft attributed to China. The malware exploited a zero day vulnerability in Microsoft's WordPad application.[85]

- The attachment sent in these email attacks contained two components: an English language carrier document that appears to be a generic contract template for a defense firm to use with a sub-contractor, and the Chinese language exploit code inserted inside the carrier document.

- When the recipient of the apparent spam email attempted to open the attached .pdf file, the file installed both the malware and a backdoor service on the targeted machine that was designed to execute the next time the user logged in.

The malware, sent in a wave of spearphishing attacks against various US companies, was intended to provide the intruder with the ability to remotely access and control the targeted computers, another common characteristic of computer network exploitation activities attributed to China.

- The newly installed service connects to an external host outside of the targeted company's network and allows the intruder to take control of the victim's machine remotely with the same access and operational capabilities as though they were sitting at the user's keyboard.

Programming bugs in the malware used during the fall 2008 campaign and the intruders' ability to quickly obtain an earlier version as a replacement program,

[85] See Microsoft Security Advisory 960906.

strongly suggests this was the first time the newer version was being used by these attackers. Their ability to obtain a replacement version quickly may be the result of having access to the developer or someone managing a repository of the developer's work. If the latter is true, it implies the existence of a support infrastructure for the individuals targeting US Government and commercial networks. However, this is still speculative and requires further research to corroborate.

- The initial version of the malware was compiled in late October 2008 and used within weeks by the intruders. This short time interval between the date of creation and first use implies that the intruder (or intruders) had the means to obtain customized zero-day malware quickly.

- When they encountered operational problems with the code, the intruders quickly obtained an older version of the malware, compiled in January 2008 and resumed their work with little delay.

Government Recruitment from Hacker Groups

Government efforts to recruit from among the Chinese hacker community and evidence of consulting relationships between known hackers and security services indicates some government willingness to draw from this pool of expertise. It does not imply that authorities have established many such relationships or intends to enlist whole groups for large attacks on US systems.

- Between July 2007 and November 2008, an individual using the screen name "City_93" posted job vacancy announcements for the Ministry of Public Security's First Research Institute (posting a Web address www.fri.com.cn) on the discussion board for EvilOctal.com and XFocus.net, two of the largest and in the case of XFocus, most established hacker forums in China.

- "City_93" eventually posted 10 vacancy notices on Evil Octal between 2007 and 2008 and on both sites engaged in lengthy discussion threads on the application procedures and nature of the job with interested users. The job postings were for entry level programmers with experience in the development and implementation of network security system projects.

- The MPS First Research Bureau provides a variety of science and technology research and development to operational elements of the MPS. The Institute has an information security research group according to its Website.

Figure 4: Job posting on hacker Website EvilOctal by a Ministry of Public Security 1st Research Institute representative looking for applicants with information security and programming backgrounds. The post was made by a user with the screen name "City_93" who self-identified as a MPS employee and used an MPS email for follow up contact.

The founding member of the influential Chinese hacker group Javaphile has a formal consulting relationship with the Shanghai Public Security Bureau and researcher credentials at the information security engineering institute of one of China's leading universities, according to an analysis of academic publications, media reporting, and research done by an independent IW analyst. Javaphile has an established history as a hacktivist group, leading attacks on the White House and other networks during the hacker wars in 2001-2002 and is still considered an active and influential group.

- The co-founder of Javaphile, Peng Yinan, using the screen name *Coolswallow,* created Javaphile while a student at Shanghai Jiaotong University's School of Information Security Engineering in 2000 according to posts he made in 2003 on a Shanghai Jiaotong student online forum that has since been removed.[86] The group initially functioned solely as a java language user group until the EP-3 incident catalyzed the members to convert Javaphile into a hacker group. The members focused on developing tools, sharing

[86] For the full analysis of the linkage between Coolswallow, Ericool, and Peng Yinan, see Scott Henderson's analysis and research posted on his blog, The Dark Visitor, available at: http://www.thedarkvisitor.com/2007/12/javaphile-buddhism-andthe-public-security-bureau/.

techniques and carrying out attacks on US Websites, according to postings the group made on a student online forum.[87]

- Independent research by a US IW specialist, Scott Henderson, linked Peng to two screen names, CoolSwallow and Ericool, that he used regularly either on his Javaphile Website or to publish essays on Buddhism on a separate Website devoted to the subject where he was a member.

- Henderson later identified Peng's Shanghai Public Security Bureau consultant credentials from a Shanghai Jiaotong University student newspaper story about a lecture that Peng, an alumni of the Information Security Engineering Institute, had given to students there called "Hacker in a Nutshell." These accounts and publicity posters also described Peng as an "experienced hacker" (see Figure 5).[88]

- Following this exposure on Henderson's blog, the Coolswallow and Buddhist society sites were taken down and little was heard in online hacker forums from Coolswallow or Ericool for over a year.

Figure 5: Poster advertising Javaphile member and Public Security Bureau consultant, Peng Yinan's 2007 lecture, "Hacker in a Nutshell" at Shanghai Jiaotong

[87] Scott Henderson, *The Dark Visitor,* April 2007, p. 36
[88] Scott Henderson, The Dark Visitor blog. The Shanghai newspaper article is available at: http://jd.sjtu.edu.cn/BKPG/xsyd/xywh/2007-11-05/1194245625d7507.html

University. His name is circled and his hacking and PSB credentials are underlined above.[89]

- Peng later published two articles in 2008 on computer network exploitation techniques under his own name and listed as an affiliated researcher at Shanghai Jiaotong University's Information Security Engineering Institute.[90]

- The Institute is currently headed by Peng Dequan, a former Director of the Science and Technology Commission of the Ministry of State Security (MSS), China's primary foreign intelligence service.[91]

The PLA in 2005 reportedly held a series of regional or provincial hacker competitions to identify talented civilians who could support military CNO requirements, according to an uncorroborated Taiwan media source referencing an article from a Sichuan university student newspaper.

- Chinese hacker, Withered Rose (aka Tan Duilin), the former leader of the prominent NCPH hacker group, allegedly won the competition in Sichuan, a story which has been repeated often in Western media reporting but is difficult to verify.

- The accounts claim that representatives from the Sichuan Military Command Communication Department apparently contacted Tan in 2005 directly and told him to participate in the network attack and defense training event organized by the provincial military command, in preparation for the coming Chengdu Military Command Network Attack and Defense Competition later that year, according to an interview conducted with him by the Sichuan University of Science and Technology student newspaper.[92] If true, the story implies that the PLA was engaged in "talent scouting" within the hacker community and organizing formal events such as this contest to aid the effort.

---

[89] See: http://jd.sjtu.edu.cn/BKPG/xsyd/xywh/2007-11-05/1194245625d7507.html

[90] The articles entitled "An Analysis of Blind SQL Injection Techniques" and "Feed Injection and Defenses in Web 2.0" published in the journal *Information Security and Communication Security* identified Peng and his co-authors (also former Javaphile members) as researchers at Shanghai Jiaotong University's Information Security Engineering Institute. Citation drawn from the Wanfang database, available at: http://d.wanfangdata.com.cn/Periodical_xxaqytxbm200805032.aspx

[91] "Computer Security Urged to Be Tightened," PLA Daily Online, English edition, August 14, 2000; available at http://english.peoplesdaily.com.cn/english/200008/14/eng200008_48117.html | OSC, CPP20060908425001001, "Wuhan University State Key Laboratory of Software Engineering," 28 August 2006.

[92] OSC, CPP20071115310002, "Tzu-Yu Shih-Pao: China Employs 30,000 Internet Soldiers," 10 November 2007| Simon Elegant, "Enemies at the Firewall," *Time Magazine,* December 6, 2007; available at: http://www.time.com/time/magazine/article/0,9171,1692063,00.html

- Interestingly, Tan was recently arrested on hacking charges when he attacked the websites of rival hacker groups.

Commercial Support to Government CNO R&D

China's long term investment in its high technology sectors is paying dividends for the PLA as they have access to increasing numbers of domestic firms able to design, build, and service advanced IT systems in support of PLA C4ISR and CNO requirements. The ability to recruit these employees into militia units is only one benefit that the government is deriving from the growth of the IT sector in China. Some firms, such as Huawei, are well known in the West and occupy significant market share in both China and abroad, but a host of other smaller firms like Venus Technologies, also provide increasingly sophisticated platforms and technology to the PLA and government security organizations.

- Huawei is a well established supplier of specialized telecommunications equipment, training and related technology to the PLA that has, along with others such as Zhongxing, and Datang, received direct funding for R&D on C4ISR systems capabilities. All of these firms originated as state research institutes and continue to receive preferential funding and support from the PLA.[93]

- ZTE Corp, another of China's large telecommunications manufacturers, and Huawei, also provide certification training and related engineering training to PLA personnel assigned to communications and IW related positions, according to provincial level Communist Party military newspapers.[94]

- Civilian IT companies have provided personnel to staff IW militia units that are tasked with both CNA and CND missions during wartime and extensive CNE missions during peacetime.[95]

- Venus Technologies Inc, which has close ties to the hacker groups XFocus and NSFocus, is also a well known provider of information security and computer network operations expertise to the PLA and dozens of other entities

[93] Evan Medeiros, Roger Cliff, Keith Crane, James Mulvenon, *A New Direction for China's Defense Industry,* RAND Corp, 2005, p. 213.
[94] OSC, CPP20090430682010, "Network 'Spiderman' – Remembering Wang Jianguo, Class 6 NCO from Certain Main Communications Station," by Gong Yun, Xia Hui, Zheng Xisheng, *Guangzhou Zhanshi Bao*, March 5, 2009, p.4.
[95] OSC, CPP20031002000138, "Building a High-quality Militia Information Technology Element," by Ye Youcai and Zhou Wenrui, PLA Guangzhou Garrison District, Academy of Military Science, *Guofang*, September 15, 2003.

> in the PRC government. Venus' customer list published on their Website includes all PLA service branches, all PLA Staff departments (i.e. the General Staff, Armaments, Logistics, and Political Departments) and the defense consortiums China North Industries Group (NORINCO, a well documented arms exporter), China Aviation Industry Corp I (AVIC I), China Aerospace Science and Technology Group (CASIC), China Shipbuilding Industry Corporation, and the Jiuquan Satellite Launch Base, China's oldest space launch facility located in Inner Mongolia.[96]

To date, the evidentiary record regarding the PLA's or other state security groups' use of Chinese hackers to conduct network exploitation activities against US networks remains highly anecdotal. Western media reports that claim that the PRC government has recruited an "internet army" from among the millions of Chinese hackers, are spurious at best. The limited reporting available from open sources, however, does suggest that some precedent exists for state security organizations to seek computer network operations expertise from individuals with sophisticated hacker skill sets. How these organizations are using the talent they recruit, the numbers of individuals involved in possible state sponsored CNO activities, and how these individuals are integrated—if at all—into ongoing cyber intelligence operations all bear careful scrutiny and continued research.

[96] List is available on Venus Tech's website located at: http://www.venustech.com.cn/aboutitem/189

Cyber-Espionage[97]

Foreign intelligence services have discovered that unclassified US government and private sector information, once unreachable or requiring years of expensive technological or human asset preparation to obtain, can now be accessed, inventoried, and stolen with comparative ease using computer network operations tools. The return on present investment for targeting sensitive US information in this way (the intelligence gain) can be extraordinarily high while the barriers to entry (the skills and technologies required to implement an operation) are comparatively low. Many countries are in the process of developing capabilities to either respond defensively to this threat or build their own offensive network operations programs, however, China is most frequently cited as the primary actor behind much of the activity noted in media reporting, and US officials are increasingly willing to publicly acknowledge that China's network exploitation and intelligence collection activities are one of this country's most consuming counterintelligence challenges.

China's development of its computer network operations capability extends beyond preparations for wartime operations. The PLA and state security organizations have begun employing this capability to mount a large scale computer network exploitation effort for intelligence gathering purposes against the US and many countries around the world, according to statements by US officials, accusations by targeted foreign governments, and a growing body of media reporting on these incidents.

A long term, persistent campaign to collect sensitive but unclassified information from US Government and US defense industry networks using computer network exploitation techniques, long attributed to China, has successfully exfiltrated at least 10 to 20 terabytes of data from US Government networks as of 2007, according to US Air Force estimates and that figure has possibly grown in the past two years, though no figure is publicly available.

[97] The content of the following section is based upon analysis of media but also upon the deep experience and insights that Northrop Grumman Corporation has gained as a major provider of information security services and its own experience defending a large, geographically dispersed enterprise. Northrop Grumman's appreciation of the nature of cyber threats directed at the United States is grounded in deep, real world experience, and the incidents and insights presented here are derived from open source research and the company's familiarity in the aggregate dealing with a variety of advanced cyber security issues. ***The incidents and adversary patterns of operation presented here should not be construed to refer to any specific company or government agency unless explicitly stated otherwise.***

General James Cartwright, while serving as the Combatant Commander of US Strategic Command, testified before a Congressional commission that China is actively engaging in cyber reconnaissance by probing the computer networks of U.S. government agencies as well as private companies. He further noted that the intelligence collected from these computer reconnaissance campaigns can be used for myriad purposes, including identifying weak points in the networks, understanding how leaders in the United States think, discovering the communication patterns of American government agencies and private companies, and attaining valuable information stored throughout the networks.[98]

A review of the scale, focus, and complexity of the overall campaign directed against the United States and, increasingly, a host of other countries around the world strongly suggest that these operations are state-sponsored or supported. The operators appear to have access to financial, personnel, and analytic resources that exceed what organized cybercriminal operations or multiple hacker groups operating independently could likely access consistently over several years. Furthermore, the categories of data stolen do not have inherent monetary value like credit card numbers or bank account information that is often the focus of cybercriminal organizations. Highly technical defense engineering information, military related information, or government policy analysis documents are not easily monetized by cybercriminals unless they have a nation-state customer, making the activity "state-sponsored" by default, regardless of the affiliation of the actual operators at the keyboard.

The scope of operational activities, deep knowledge of the targeted networks, and volume and topics of data exfiltrated suggest that the attackers are supporting consumers involved in defense related engineering research, policy specialists interested in US-China relations, and military planners gathering intelligence on US military information systems and operations.

US Government officials assess that this activity, in the aggregate, has the potential to erode the United States' long term position as a world leader in S&T innovation and competitiveness and the collection of US defense engineering data has possibly saved the recipient of the information years of R&D and significant amounts of funding.[99]

---

98 "China's Military Modernization And Its Impact On The United States And The Asia-Pacific," Hearing before The U.S.-China Economic And Security Review Commission, March 29-30, 2007, p. 7; Available at http://www.uscc.gov/hearings/2007hearings/transcripts/mar_29_30/mar_29_30_07_trans.pdf

99 Jeff Bliss, ''China's Spying Overwhelms U.S. Counterintelligence,'' *Bloomberg,* April 2, 2007. | Shane Harris, "China's Cyber-Militia," The National Journal, Saturday, May 31, 2008, available online at: http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php

These operations are succeeding in part because current industry and US government information security paradigms are largely based on reactive controls such as traditional signature-based anti-virus vendor models, common host and network defensive measures that are often inadequate against advanced attackers. When a product vendor or the research community discloses new security vulnerabilities, security software vendors rapidly analyze it and produce "signatures," or encoded representations of the anticipated effects of an attack against this new vulnerability. These signatures are applied to network control devices such as Intrusion Detection and Prevention Systems (IDS/IPS) and firewalls, and on individual computers as anti-virus rules or host IDS/IPS signatures. Adding signatures proactively to these systems without prior knowledge of a vulnerability or possibly an observed or lab-generated sample attack, is difficult and often discouraged.

- Many organizations are reluctant to patch systems and software against vulnerabilities for which there have not been publicly released exploits. Larger organizations with more mature security practices or resources often use complex behavioral signatures, or models, applied to Security Event and Information Management (SEIM) or Network Behavioral Analysis (NBA) systems but these techniques are usually fed by component signature-based systems, they, too, suffer the same shortcomings.

- NBA systems show greater promise when tuned to look for anomalous behavior, however, there is generally much greater administrative overhead and a high false alarm rate in this mode.

- Traditional network and system management is a balancing act of performance, expense and security and common wisdom dictates a certain hesitance to make changes on functioning, often critical, systems.

These operators exploit this reactive defense model and they have the resources necessary to develop and exploit previously unknown vulnerabilities that are often are missed by signature-based IDS/IPS and endpoint protection software. The Chinese academic community and hacker groups—like many hacker groups around the world—are heavily focused on researching new zero-day vulnerabilities.

- Anecdotal reporting from information security industry sources suggest that Chinese researchers are also willing to purchase zero day attack tools from third party sources, though this has not been independently corroborated.

- Zero day exploits are bought and sold in numerous public and private markets without the involvement of the victim software's vendors, often for tens of thousands of dollars per vulnerability.[100]

The overall effort likely consists of multiple groups and skilled individuals operating against different targets given the high operational tempo and diversity of targeting observed to date (see Timeline of Alleged Chinese Intrusions below). These operators, some possibly affiliated with PRC government or military organizations and others probably freelance hackers, have access to software developers capable of developing zero day exploits and using tools that are often created on computers with Chinese language settings or Chinese language developer kits.

- The adversaries associated with this issue are successful because they are able maintain a presence on a targeted network for extended periods enabling them establish a connection to a compromised computer on the network when operationally required for activities such as reconnaissance of the network topology, determining where high value information resides, or to conduct social and professional network analysis to support future spearphishing campaigns.

- This latter information is exploited most frequently to craft specific, seemingly legitimate-looking, emails to targeted users often referencing a current project or meeting with which the recipient is involved. The emails usually contain either malicious software embedded in an attachment or links to malicious Websites.[101]

- The scale and complexity of targeting associated with this effort suggests that it is probably backed by a mature collection management bureaucracy able to collate and disseminate collection priorities to diverse teams of operators, intelligence analysts, and malware developers. These individuals are likely a mix of uniformed military personnel, civilian intelligence operators, and freelance high-end hackers.

These types of attacks often begin with an email message with a file attached containing both the exploit code and another small piece of software which will give the attacker control of the victim's computer. When this file, usually an image,

---

[100] See for example: http://www.securityfocus.com/columnists/470 and http://www.eweek.com/c/a/Security/Hackers-Selling-Vista-ZeroDay-Exploit/ for additional background.
[101] Brian Grow, Keith Epstein and Chi-Chu Tschang, "The New E-spionage Threat," *BusinessWeek*, April 10, 2008, available online at: http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

document, or spreadsheet is opened by the vulnerable program on the victim's computer (e.g. Powerpoint, Wordpad, Adobe Acrobat, etc), the backdoor program executes. Email is the most common entry vector because the operators are often able to learn an employee's (or group of employees') trust relationships (i.e. their professional networks) by analyzing who they frequently email. The intruders then craft credible looking emails from members or groups within an individual's network that the target will likely open. [102]

Date: Tue, 10 Dec 2008 06:58:13 -0700 (PDT)
From: John Doe <john.q.googdguy@yahoo.com>
To: employee.name@companyname.com

Subject: 7th Annual U.S. Defense Conference

7th Annual U.S. Defense Conference
1-2 Jan 2009

Ronald Reagan Building and International Trade Center
Washington, DC

Download 2009 Conference Preliminary Program (PDF)
http://conferences.satellite-stuff.net/events/MDA_Prelim_09.zip

Download 2009 Conference Registration Form (PDF)
http://conferences.satellite-stuff.net/events/MDA09_reg_form.zip

Contact: John Doe
Contractor Information Systems
(703) 555-1234
john.doe@yahoo.com

Figure 6: A sample of an attack email that was sent simultaneously to many US commercial firms. The identifying information and the conference have been modified from the original.

The conference referenced in the email sample in Figure 6 was legitimate, but the linked download site was not. The registration form and program files, when downloaded and unzipped, gave the attacker complete remote control of the targeted user's computer. The operators tasked with targeting had previously identified this company's employee and all of the other recipients, as someone likely to be interested in the subject of the email and download the form by surveying his or her online presence: conference attendee lists, subscriptions to newsgroups, social networking sites such as Facebook and Linkedin, and corporate public affairs releases.

[102] Brian Grow, Keith Epstein and Chi-Chu Tschang, "The New E-spionage Threat," *BusinessWeek*, April 10, 2008, available online at: http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

- The operators often reuse the employee's profiles generated by this reconnaissance in multiple targeting attempts either because the user failed to open the attachment the first time or simply because they are an "easy mark" who usually opens these emails and thus represent a reliable entry vector for the intruders.

- This initial penetration with email and malicious attachment is frequently only the first phase of an advanced operation as the users targeted first and the data on their computers are often not the actual target of collection. Targeting the data owners of the attacker's actual collection objective increases the risk of detection and possible implementation of tighter controls around the data they are seeking to exfiltrate, making later attempts more difficult.

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.

Reasons for using different individuals or groups could be due to the specialized skills required for each phase of an intrusion or perhaps for "compartmentation" reasons: the first team or operator does not need to know the details of what is being targeted by the second team or operator, thus ideally, improving overall operational security. 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.

- 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.

- Operators have also attacked mobile users' virtual private network (VPN) software, which allows employees of a company to access their corporate network while outside of the office. Operators have modified VPN software to allow access back into the network through the remote user's systems. Attackers have on occasion installed additional network software to mask their remote control communications, such as encryption rootkits that hide the attackers' presence from legitimate system administrators.

- All of these steps help ensure long-term access to the target organization's network and help provide freedom of movement to the attackers once inside the network.

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. The attackers in these operations 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 "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 often 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, ensuring that investigators are unable to identify the data's final destination.

China's defense industry is producing new generations of weapon platforms with impressive speed and quality, and while these advancements are due to a variety of domestic factors, Chinese industrial espionage is providing a source of new technology without the necessity of investing time or money to perform research. Computer network exploitation in support of these collection requirements has possibly expanded the range and detail of information available for collection in a way that previously required close HUMINT-enabled access to obtain the data (e.g. an agent inside or close proximity to a US citizen and their laptop or other electronics). Chinese espionage in the United States, which now comprises the single greatest threat to U.S. technology, according to US counterintelligence officials,[103] is straining the U.S. capacity to respond. This illicit activity both from traditional techniques and computer-based activity are possibly contributing to China's military modernization and its acquisition of new technical capabilities.

[103] *2007 Report to Congress of the US China Economic and Security Review Commission,* November 2007, p. 7., available at: http://www.uscc.gov

Operational Profile of An Advanced Cyber Intrusion

The following case study is based wholly upon an internal post-incident forensics investigation and discussions with information security specialists from a single affected firm following a penetration and data exfiltration by intruders likely associated with a state sponsored operation. The company's internal analysis of the incident indicates that the attacks came through, or originated from, China and many of the techniques are consistent with the operational profile attributed to other attacks believed to originate from China. This case study reflects the details of only a single incident. Private sector firms—even within a given industry—frequently employ a variety of information security tools and strategies based on their unique network architecture and approaches to risk management.

Information security analysts at a large US commercial firm several years ago detected a high volume of data being sent from their network to multiple computers in the US and overseas, with many aspects of the activity matching the profile often associated with other state sponsored attacks. The analysts quickly began putting blocks in place on their network to halt the data loss but not before significant volumes of data were lost to the intruders.

The scale of this operation, which also targeted other large US companies within a several week period suggests a disciplined command and control structure, a means of sharing specific data collection requirements for various targeted companies and the capability to collate and process extremely large volumes of data once exfiltrated. Additionally, in this specific incident at least, the attackers selected the data for exfiltration with great care. Though they had the opportunity, they did not simply "take what they could get" and leave, rather, they chose specific files, often ignoring related information in adjacent directory locations, activity which suggests these attackers were disciplined and operating from a specific list of collection requirements, a characteristic usually only found in highly professional operations.

During the incident described below, the attackers did not open and review file contents—though they had the required file permissions—but instead navigated immediately to the files or folders they wanted and began the steps necessary to exfiltrate them, suggesting that they had reviewed the directory contents offline and that they had already gained access to this firm's network to conduct detailed reconnaissance, including the possible exfiltration of file directory listings.

These types of operational techniques are not characteristic of amateur hackers operating in widely dispersed geographic areas. While the affiliation of the individual operators is impossible to establish, the coordination required to stage this operation suggests that even if these were freelance operators not directly affiliated with a state or military organization, they had professional quality organization and discipline and a specific set of collection objectives, evidenced as much by what they *didn't* take—

despite having easy access to the data—as what they did take. The type and specificity of data stolen in this case also suggests that the end users were already identified and that they likely had deep science and technology resources at their disposal to make use of the stolen information.

While attribution is always the most difficult component of information security investigations, hackers—individuals and groups alike—tend to operate in a consistent manner, exhibiting a preference for specific tools, possess a unique keyboard presence,[104] and often tend to target the same types of data across their targets. This case is consistent with other incidents attributed to Chinese intrusions into US networks though no firm attribution data was available from this case.

Over a multi-day period during this incident, intruders staged a complex data exfiltration operation and while the activity associated with this incident occurred within a relatively short span of time, the preparations and reconnaissance necessary to support it had likely been ongoing for months. The teams or individuals who carried out this operation displayed discipline and a deep knowledge of the network architecture they targeted, suggesting that these operators had likely spent months patiently assembling a detailed picture of this network.

- Identical remote communication and administrative tools and operational techniques were used in earlier incidents with this and other companies; they operated at times using a communication channel between a host with an IP address located in the People's Republic of China and a server on the company's internal network, a technique observed consistently in similar intrusions at other commercial firms.

- Analysis of the operation suggests that the adversaries previously identified specific directories, file shares, servers, user accounts, employee full names, password policies, and group memberships on the network, likely during their detailed reconnaissance phase.

- They did not open any files to review the contents prior to exfiltration, suggesting they already knew the contents or at a minimum, the file names of the data they were tasked with stealing.

[104] An individual's "keyboard behavior" in the context of computer network intrusions refers to the specific habits that a hacker might develop over the course of performing certain functions many times. The sophistication, frequency, combination of commands, and elapsed time between keyboard entries can all help in the creation of a "forensic profile" an individual attacker.

The adversary used at least two groups in the operation; a breach team (referred to by these information security analysts as "Team One") and a collection team (known as "Team Two"), responsible for gathering and exfiltrating the targeted data.

- Each team employed distinct toolkits and used them in unique ways suggesting not only different operational goals but also different individuals at the keyboard.

- The teams maintained a base of instrumented hosts on the company's network that they held in reserve for use as required at external locations to support their covert communications for an extended period of time.

Prior to this data exfiltration, the company's information security analysts had detected activity attributed to these types of sophisticated attackers, but it was generally characterized by low volumes of traffic through compromised hosts and appeared primarily focused on maintaining access and presence. The company's information security staff detected and countered these compromises in the months prior to the final data exfiltration, however, the attackers' appear to have simply created new entry vectors or reverted back to other pre-established means of accessing the company's network. The reconnaissance phase seems to have been sufficiently methodical and quiet to permit the compilation of an accurate map of the network over time. The adversary identified servers, file shares, individual employees, user groups, and the credentials necessary to support a complex data exfiltration operation later.

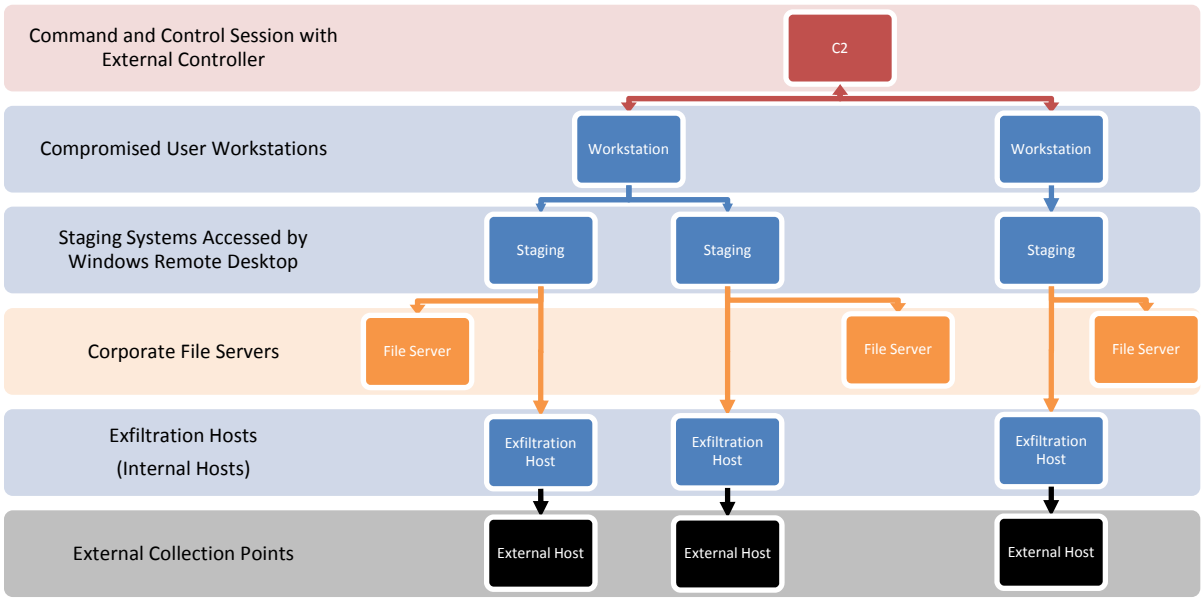


Figure 7: Diagram of the data exfiltration operation attributed to a sophisticated—possibly state sponsored—intrusion into a US commercial network.

Intruder Command and Control Infrastructure

Analysis of the intruders' activity prior to, and during, the exfiltration operation indicates that their command and control architecture relied upon previously stolen valid user accounts to authenticate to the company's internal servers. Once authenticated, they established communications with a variety of previously compromised computers inside the company's network. The operators then tunneled Remote Desktop Protocol (RDP) within their existing communication channels to establish contact with the targeted hosts for purposes ranging from maintaining basic access to the control of the eventual data exfiltration. Additional stolen account names and passwords were used as needed to gain access to otherwise protected resources such as computers, network shares, folders and files.

- Analysis of proxy logs and forensic data revealed that the operators used dozens of employee accounts on almost 150 occasions to access the network in the days leading up to the exfiltration.

- At times, they used highly privileged administrative accounts and passed NTLM hashes in lieu of passwords directly to the proxy authentication mechanism.[105] The use of password hashes, which were harvested directly from compromised domain controllers, appears designed to defeat any two-factor authentication (T-FA) techniques that may have been in place to defend against brute-force password cracking tools.

- The use of NTLM hashes, which were harvested from domain controllers using password collection tools, appears designed to defeat any multifactor authentication techniques that may have been in place to defend against brute-force password cracking tools.

- The adversary also repeatedly enumerated group membership of accounts in the organization's primary domain, which assisted them in the identifying which employee accounts to use when trying to access files restricted to certain users.

[105] Many proxy servers can be configured to require an NTLM challenge/response authentication before access is granted to the protected resource, such as Internet/WWW/FTP access. If an attacker is in possession of the authentication hashes, they can use the hash directly, rather than first "crack" the password, then re-hash it for the authentication service.

Movement of Targeted Data to Intermediate "Staging Servers"

During the first several days of this incident, the adversary transferred the data selected for exfiltration from company file servers (where it normally resided) to Microsoft Exchange email servers that acted as intermediate staging points (See Figure 7, the transfer occurred between the Staging Systems and the Corporate File Servers in this diagram). Their reconnaissance of the network enabled them to select servers that offered the highest performance and network throughput. The identification and selection of these servers, again, underscores the adversary's precise knowledge of this network's architecture, gained from detailed reconnaissance prior to this operation.

The attackers began the preparations for moving data from the files servers to the staging points by establishing clear lines of command and control and identifying the appropriate hosts to use for the staging and exfiltration phases of the operation. Analysis of the available data indicates that the adversaries, using standard Windows file transfer tools, moved targeted data from the shares to the staging servers.

- Operators likely associated with the collection team (Team 2), using an internal host as a C2 node, established multiple connections through encrypted RDP sessions to various internal email servers prior to staging data on these machines.

- Forensic data revealed an increase of short duration communications between the internal hosts used as C2 nodes and email servers in the days prior to the staging operation. This process was likely to identify and confirm the resources that would be used in all phases of the subsequent operation.

- Concurrent with this activity, the adversaries also established communications between the email servers used for the exfiltration operation and an external Website that was likely under their control. The attackers used this as their primary C2 channel to control at least seven of the internal email servers while they prepared their operation (see the external drop points in Figure 7).

After moving data to staging servers, the operators renamed all targeted files with nondescript labels to resemble a legitimate Windows application likely selected to appear innocuous on the staging servers.

- Once the transfer to staging servers was complete, the attackers encrypted and compressed the files into numbered volumes of RAR archives—all

exactly the same size—in preparation for exfiltration.[106]

- Information security analysts within the company noted that the tools and techniques used for this process closely matched that used in previously detected activity on the organization's network, confirming either that this was the same entity or that operators responsible for different intrusions have a means of sharing data about their targets or activities.

Exfiltration of Data from the Internal Network

Reflecting their methodical preparations, these operators used seven servers almost in tandem to move data out of the company's network, suggesting that speed was a priority during this phase of the operation. The movement of data out of the internal network is the most vulnerable phase of the entire operation because of defensive tools the company had in place on its network perimeter and was the only point that they were detected during their multi-day presence in the network in preparation for this action.

The final stage of the exfiltration operation began in the evening (local time for this firm), after all of the targeted data was staged on the intermediate hosts. Prior to starting the exfiltration, the operators prepared with characteristic care: establishing an overarching C2 channel, testing their connections, possibly rehearsing their procedures, and checking their available bandwidth before beginning the actual exfiltration.

- After the commencement of the exfiltration from a single email server, operators enumerated all of the email servers in the targeted areas. This was significant because their request used the company's standard internal naming convention for these servers in the geographic area where the servers were located, knowledge that is obtained only through highly detailed reconnaissance of the network.[107] The command returned a list of several dozen servers, 75 percent of which they used in the operation as either staging or exfiltration points.

- The teams involved in the operation prepared for the actual exfiltration by

[106] Of note, the RAR archives were all exactly 650MB in size, the maximum capacity of a standard CD ROM, indicating a possible future storage or transfer medium.
[107] Organizations with networks dispersed over large geographic regions often use a naming convention for their servers that identifies the physical location of the server, followed by internal company organizational details or a code to represent the server's role, e.g. a print server located in Montana in the XY Division may be internally named "MTXYP012." In this case, the attackers knew the exact convention that their target used and searched for all of the servers in the geographic area where their targeted data was located.

directing each of the servers that would be used to move data out of the company to access a large video file (over 20MB) from an internal server not otherwise targeted or involved in the overall operation. In each case, the connection was terminated by the attackers after receiving only a short portion of the video. This truncated downloading suggest they were not attempting to view the contents of the file itself, but likely testing the available bandwidth for transporting large volumes of data.

The attackers, operating with a valid user account, controlled one of the company's desktop machines which they used as a C2 node to direct the multiple servers involved in the overall exfiltration operation (the company's analysts identified a total of four desktop machines used as C2 nodes). This particular C2 node connected to multiple internal servers, including one staging server, two other known intermediate hosts, and an external IP address located in the United States.

- One of the internal C2 hosts established a connection to a DSL customer of a commercial US-based Internet service provider. This proxy connection remained open for the entire exfiltration phase. During that time, this node connected via RDP into at least eight external hosts, one of which was located in Hong Kong.[108]

- Forensic analysis of the traffic flow in this incident indicates that the attackers moved large volumes of data from the staging servers to those used as a forwarding point for exfiltration out of the company's networks (the connection between "Exfiltration Hosts" and "External Drop Points" Figure 7).

The Team One operators responsible for penetrating the information security defenses possibly rehearsed their portion of the operation using innocuous files prior to actually commencing the data exfiltration, then attempted to send three RAR archive files via independent FTP sessions.

Analysis of the operators' command channel activity indicates that they encountered serious problems with two external hosts intended to receive data exfiltrated from this company's network. They also attempted custom FTP client and server software, but it failed for unknown reasons. The operators abandoned one of these servers and the custom FTP software, likely due to the slow and unreliable data transfer rates, and continued with standard FTP server software running on five more reliable remote hosts for the remainder of the data exfiltration.

[108] The Hong Kong connection was unsuccessful and probably accidental given the careful steps taken to use US-based servers to receive the data once it started flowing. The probable accident does potentially identify one of the adversary's external resources, possibly used to receive data from the US servers once the operation was complete.

- On the final day of the operation, at approximately the same time in the evening that they started each day previously, the operators established an FTP connection from one of the internal exfiltration servers to an external host. They verified that their communication channel was working properly by uploading a zero byte file followed by a much larger file. Apparently satisfied that this connection functioned properly, the operators logged out of this internal server.

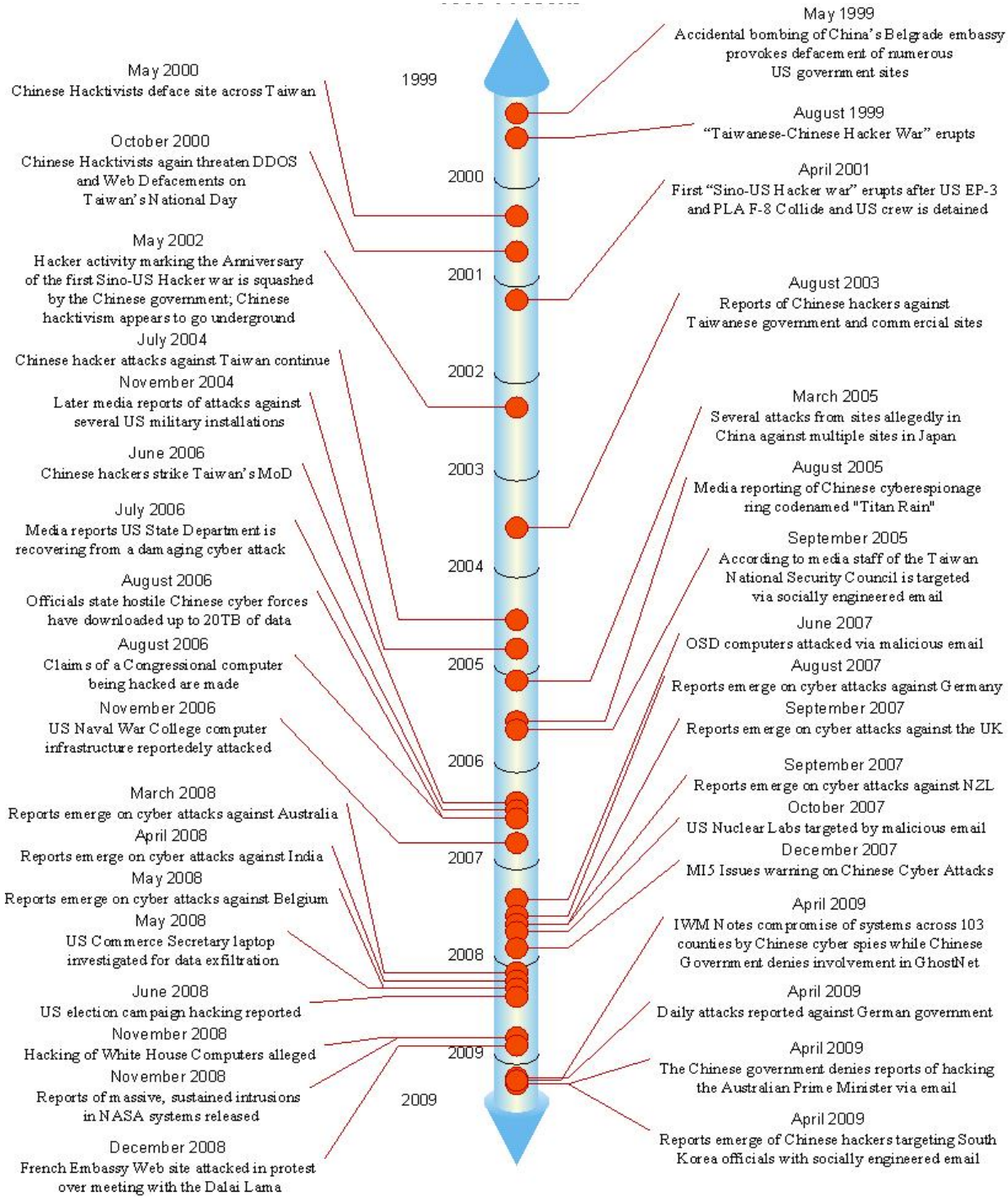
- The operators reconnected within half an hour to this same internal server, and using the same credentials attempted to move the first encrypted RAR file containing the company's proprietary data. Two minutes later, they attempted to move another file, and then logged out. Minutes later, they reconnected and attempted to move a third file. In each instance, the FTP connections terminated prematurely for unknown reasons. It appears that while small file transfers were successful across this channel, large file transfers caused it to fail.

- They then attempted to transfer files to a new remote FTP server using custom FTP software that provided an additional layer of encryption. The attacker's FTP software implemented a custom command, "SORT", issued by the client and recognized by the server as a signal to receive encrypted communications in lieu of a normal, unencrypted, file transfer. This same software was then tried almost immediately on a new remote host, and again it failed to complete a test transfer. In a final test, they connected back to their first remote server which was now running their custom FTP server software, and attempted a transfer; it too failed.

- They then connected to a second US university and succeeded in manually moving large RAR files using unmodified FTP server software. Shortly thereafter, the operators established a series of automated, redundant, transfers to five remote hosts, all running this same server software, in an effort to maximize the success rate of this main data exfiltration effort.

The information security staff eventually detected and blocked the exfiltration in mid-stream but not before significant amounts of company data left the network. Intrusion prevention systems on the company's network were then tuned to alert and block further activity and for the next five hours these systems continued to detect attempts by the operators to return, suggesting that they were interrupted before completing the full exfiltration as planned. Information security analysts with this firm have no means of determining the total intended size of this exfiltration operation.

Timeline of Significant Chinese Related Cyber Events 1999-Present



Chronology of Alleged Chinese Computer Network Exploitation Events Targeting US and Foreign Networks

1999

May 1999: The accidental US bombing of China's Serbian embassy in May 1999 draws angry protest from China's hacker community and leads to a series of defacements of US government Websites by Chinese hackers.[109]

August 1999: The "Taiwan-China Hacker War" erupts after then-President of Taiwan Lee Teng-hui recommended Taiwan's relationship with the People's Republic of China be on a "state-to-state" basis. Chinese hackers defaced numerous Taiwan government, university and commercial sites. Taiwan hackers attacked back, defacing Chinese government Websites with pro-Taiwan language.[110]

2000

May 2000: Chinese hackers deface Taiwan government Websites with anti-Taiwan political statements in protest over the swearing in of Chen Shui-bien.[111]

October 2000: Chinese hackers threaten a denial of service attacks and Web defacement against Taiwan government and private Websites in protest over Taiwan's celebration of National Day.[112]

2001

April 2001: The collision of a US Navy EP-3 reconnaissance plane and a People's Liberation Army Navy (PLAN) F-8 fighter and the subsequent detention of the EP-3 crew members for eleven days on Hainan Island sparked the first "Sino-US Hacker

[109] Ellen Messmer, "Kosovo Cyber-War Intensifies: Chinese Hackers Targeting US Sites, Government Says," *CNN.com*, May 1999.
[110] Fred Jame, "China, Taiwan in Web Hacking 'War'," *MacWeek.com*, August 1999.
[111] "Chinese Plan To Hack Into Taiwan Websites," *The Straits Times*, October, 2000.
[112] Ibid

War," with denial of service attacks and Web defacements launched from both sides against government and private sites.[113]

2002

May 2002: To mark the one year anniversary of the first Sino-US Hacker War, Chinese civilian hackers begin to plan a large scale attack of US Websites. Their planned attacks end after the Communist Party issues a strongly worded condemnation of patriotic hacking against foreign networks.[114]

2003

August 2003: Hackers operating from sites in mainland China's Hubei and Fujian Provinces penetrate thirty Taiwan government agencies and at least twice as many Taiwan companies. The attacks focus on the Defense Ministry, Election Commission, and the National Police Administration among others. This is part of an ongoing series of attacks against the Taiwan government and private industry that continue through 2004 against other notable Websites such as Taiwan's Ministry of Finance and the Kuomintang Party.[115]

2004

June-July 2004: Attacks against Taiwan continued in 2004 targeting Websites belonging to Taiwan's Ministry of Finance, the Kuomintang Party, the Democratic Progressive Party (DPP) and the Ministry of National Defense's (MND) Military News Agency.[116]

[113] Tang, Rose, "China Warns of Massive Hack Attacks," *CNN*, May 2001
[114] Pamela Hess, "China Prevented Repeat Cyber Attack on US," *UPI*, 29 October 2002.
[115] Wendell Minnick,"Taiwan Faces Increasing Cyber Assaults," *Army Times Publishing*, June 2006.
[116] Ibid.

November 2004: US media reports that Chinese hackers attacked multiple unclassified US military systems at the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona, the Defense Information Systems Agency in Arlington, Virginia, the Naval Ocean Systems Center in San Diego, California and the United States Army Space and Strategic Defense installation in Huntsville, Alabama.[117]

2005

May 2005: A series of attacks believed to have originated from China and South Korea hit numerous Japanese university and industrial Websites. The attacks may have been caused by a rise in tensions between the countries over the Japanese Education Ministry's alleged omission of key historical facts pertaining to Japan's actions in World War II and China's opposition to Japan's attempt to be a permanent member of the UN Security Council.[118]

August 2005: Media reporting first covers the story of a Chinese computer network exploitation operation codenamed "Titan Rain," alleging the intrusions into DoD systems date back to 2003. [119]

September 2005: According to Taiwanese media, the Taiwan National Security Council is targeted via socially engineered emails containing malicious attachments, infecting the recipient hosts and possibly installing a backdoor through which the intruders can return undetected. Subject lines include "arms procurement" and "freedom."[120]

2006

June 2006: Taiwan media reports that Chinese hackers attacked Taiwan's Ministry of National Defense (MND) and the American Institute in Taiwan (AIT). The attacks may have been launched using socially engineered email and attempted to spread misinformation about the MND in an apparent smear campaign. Attackers also

[117] Tom Espiner, "Chinese Hackers US Military Defenses," *Silicon,com*, November 2005.
[118] Anthony Faiola, "Cyber Warfare: China vs. Japan," *MSNBC News*, May 2005.

[119] Bradley Graham, "Hackers Attack Via Chinese Web Sites," *The Washington Post*, August 2005.
[120] "NSC Computers Targeted in Hacker Email Attack," *Liberty Times,* September 2005.

stole account login credentials from Chunghwa Telecom's Web mail system, the MND's telecommunications provider.[121]

July 2006: US media reports that intruders penetrate the US Department of State (DoS) networks, stealing sensitive information and user login credentials, and install backdoors on numerous computers, allowing them to return to the systems at will. DoS systems administrators are forced to limit Internet access until the investigation is completed. While China's involvement is not obvious, problems were especially acute at the Bureau of East Asian and Pacific Affairs, responsible for policy coordination on China, North Korea and Japan.[122]

August 2006: Pentagon officials state hostile civilian cyber units operating inside China have launched attacks against the NIPRNET and have downloaded up to 20 terabytes of data.[123]

August 2006: A Member of Congress who is a vocal critic of China's human rights record claims Chinese hackers penetrated his office computers and those of their staff.[124]

November 2006: Chinese hackers attack the US Naval War College computer infrastructure, possibly targeting war game information on the networks. The College's Web and emails systems are down for at least two weeks while the investigation takes place.[125]

2007

June 2007: Media reports indicate approximately 1,500 computers are taken offline following a penetration into the email system of the Office of the Secretary of Defense (OSD).

---

[121] Wendell Minnnick, "Taiwan Faces Increasing Cyber Assaults," *Army Times Publishing*, June 2006
[122] "Large-Scale Hacking Discovered at State Department," *Buzzle Staff and Agencies*, July 2006
[123] Dawn Onley, Dawn and Patience Wait, "Red Storm Rising: DoD's Efforts to Stave Off Nation-State Cyber Attacks Begin with China," *Government Computer News*, August 2006.
[124] Steven Schwankert, "US Congressmen Accuse China of Hacking Their Computers," *IDGNS*, June 2008.
[125] Ibid.

August/September 2007: German media reports that Berlin authorities believe Chinese hackers, with ties to the PLA, installed backdoor applications in various systems using Microsoft Word and PowerPoint documents. Targeted German government entities include the Federal Chancellery, the Ministry of Economics and Technology and the Federal Ministry for Education and Research. German officials estimate that 60 percent of cyber attacks hitting Germany emanate from China, many from the cities of Lanzhou, Guangdong, and Beijing.[126]

September 2007: UK media reports on Chinese hacker attacks against government offices of the United Kingdom, including the Foreign Office. The attacks did not lead to major adverse effects, according to officials, though the constant, ongoing activity of China's cyber attackers is acknowledged as a constant problem. [127]

September 2007: New Zealand's secret service suggests possible Chinese government involvement in the recent cyber attacks. China's government denies any involvement. This follows similar reporting regarding attacks against United States allies. [128]

October 2007: US media reports that China is suspected as the source of at least seven versions of socially engineered email targeting 1,100 employees at the Oak Ridge National Lab in Oak Ridge, Tennessee. Eleven staff possibly opened the malicious attachment, allowing the attackers to gain access to, and potentially steal, sensitive data, including a database at the nuclear weapons laboratory housing personnel records going back to 1990.[129]

December 2007: The British domestic intelligence service, MI5, issues a confidential alert to 300 chief executives, accountants, legal firms and security chiefs warning of cyber attacks and electronic espionage sponsored by Chinese state organizations. Included is a warning that the PLA is targeting businesses working in China and using the Internet to steal confidential business information.[130]

2008

[126] Ulf Gartzke, "Outrage in Berlin Over Chinese Cyber Attacks," *The Weekly Standard,* August 2007.
[127] Richard Norton-Taylor, "Titan Rain: How Chinese Hackers Targeted Whitehall," *The Guardian*, September 2007.
[128] Liam Tung, "China Accused of Cyber Attacks on New Zealand," *CNET News*, September 2007.
[129] "China Suspected in Hacking Attempt on Oak Ridge National Lab," *Homeland Security Newswire,* December 2007.
[130] Rhys Blakely, Jonathan Richard, James Rossiter, and Richard Beeston, "MI5 Alert on China's Cyberspace Spy Threat," *The Times*, December 2007.

March 2008: Australian security agencies acknowledge that they have been the victim of ongoing cyber attacks, but stop short of accusing China.[131]

April 2008: Indian officials claim China is behind "almost daily attacks into the networks belonging to the government and Indian's private sector."[132]

May 2008: The Belgian Government reports government systems have been targeted multiple times by hackers operating from China.[133]

May 2008: U.S. authorities investigate claims that Chinese officials surreptitiously copied the contents of a US government laptop during then- Commerce Secretary Carlos Gutierrez' visit to China.[134]

November 2008: Media sources report that Chinese hackers penetrate the White House information system on numerous occasions, penetrating for brief periods before systems are patched.[135]

November 2008: *Business Week* magazine publishes a report on significant cyber intrusions dating back several years at some of NASA's most critical sites including the Kennedy Space Center and Goddard Space Flight Center. The operations to prevent the attacks from China are codenamed, "Avocado." Attacks included socially engineered emails launched at top officials. Among the data stolen are operational details of the Space Shuttle including performance and engine data.[136]

December 2008: Chinese hackers associated with hack4.com stage politically motivated Web defacements on French Embassies in the US, United Kingdom, China, and Canada after French President Sarkozy's December 2008 visit with the Dalai Lama.[137]

2009

[131] Ross Peake, "Australia Confirms Cyber Attacks," *Canberra Times*, March 2008.
[132] Dan Goodin, "India and Belgium Decry Chinese Cyber Attacks," *The Register*, May 2008.
[133] Ibid.
[134] Steven Schwankert, "US Congressmen Accuse China of Hacking Their Computers," *IDGNS*, June 2008.
[135] Ibid
[136] Keith Epstein and Ben Elgin, "Network Security Breaches Plague NASA," *BusinessWeek*, November 2008.
[137] Asian News International, "French Embassy Web Site in China Hacked," *HT Media Limited*, December 2008.

March 2009: A Canadian research team publishes a study of the GhostNet cyber espionage network that targeted over 1,300 hosts around the world including those at the German, Indian, Pakistani and Portuguese embassies around the world and the Tibetan Government in Exile in India. The Canadian-based Information Warfare Monitor (IWM) notes the compromise of numerous government and private information processing systems across 103 countries. The operators responsible for the network all operated from Hainan Island in China. The Chinese government denies all accusations of responsibility or state sponsorship.[138]

March 2009: The Philippine Daily Inquirer publishes a report citing the GhostNet study's assertion that the computer network of the Philippines' Department of Foreign Affairs (DFA) has been hacked by cyber spies based in China.[139]

April 2009: Media reports the German government records daily attacks against its networks, many from Chinese based operators. the German Foreign Office is heavily targeted the reports note and are penetrated via socially engineered email.[140]

April 2009: Australian media reports that Chinese cyber spies are targeting the Australian Prime Minister via email and mobile phones. The Chinese government denies all accusations.[141]

April 2009: Media sources report that hackers based in China infiltrated the Intranet of South Korea's Finance Ministry, causing concern over the potential theft of sensitive government data. The cyber attackers used socially engineered emails to target ministry staff. The email, disguised to look as though sent from one or more trusted officials, executed malicious software when opened allowing the attackers to access the systems.[142]

---

[138] John Markoff, "Vast Spy System Loots Computers in 103 Countries," *New York Times,* March 28, 2009, http://www.nytimes.com/2009/03/29/technology/29spy.html.
[139] Aning, Jerome and Olchondra, Riza T., "RP Gov't Websites Vulnerable to Hacking," *Philippine Daily Inquirer*, March 2009
[140] John Goetz, and Marcel Rosenbach, "Cyber Spies: 'GhostNet' and the New World of Espionage," *Speigel Online*, April 2009
[141] The Australian Online. "Chinese Diplomat Dismisses Australian 'Cyber Espionage' Claims," April 2009
[142] "China-Based Hackers Access S. Korean Finance Ministry's Intranet," *AsiaPulse News*, April 2009.

Commonly Used Acronyms

AMS	Academy of Military Science
ASAT	Anti-Satellite
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CEME	Complex Electro-Magnetic Environment
CMC	Central Military Commission
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CONUS	Continental United States
EW	Electronic Warfare
GSD	General Staff Department
INEW	Integrated Network Electronic Warfare
ISR	Intelligence, Surveillance, and Reconnaissance
IW	Information Warfare
NIPRNET	Non-classified Internet Protocol Router Network
PLA	People's Liberation Army
TRB	Technical Reconnaissance Bureau
USPACOM	US Pacific Command
USTRANSCOM	US Transportation Command

Glossary of Technical Terms

Backbone – A primary transit network or series of networks, designed to carry data between different local area networks. A backbone generally has greater data carrying capacity, or "bandwidth", than the networks connected to it. The Internet Backbone is the interconnection of high-speed networks, primarily government, commercial telecommunications and academic networks that route data for public Internet users.

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.

Black hat - A computer hacker who is intent on causing damage or taking other unauthorized or illegal actions against a victim.

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

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

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).

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 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.

File Transfer Protocol (FTP) - A standard Internet protocol implemented in FTP server and client software, including most web browsers. It is used to "transfer data reliably and efficiently." http://www.rfc-editor.org/rfc/rfc959.txt

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 sub-categories: 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 sub-categories as above. Their goal is also profit (See: http://www.us-cert.gov/control_systems/csthreats.html).

Hypertext Transfer Protocol (HTTP) – The message format and exchange standard used by web browsers and web servers.

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.

INFOCON - Information Operations Condition (INFOCON) classifications mirror Defense Conditions (DEFCON) Alert System and are a uniform system of five progressive readiness conditions– INFOCON 5 thru INFOCON 1 with INFOCON 5 being a level of normal readiness and INFOCON 1 a level of maximum readiness, implemented because of severe threat or attack. As the INFOCON levels increase, elements of network functionality or services deemed lower priority or at high risk of attack may be temporarily suspended. Thus, CNA tools that work during a normal state of readiness may be rendered ineffective if the services or applications they exploit are turned off.

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.

Intrusion Prevention System (IPS) – An inline system or software that applies IDS-style logic and approves or rejects network traffic, program and data access, hardware use, etc.

Network Behavioral Analysis (NBA) – An intrusion detection system that models network traffic and alerts on violations of known acceptable activity. Rules can include data volume, time of day, traffic rate, communication partners, content, and other elements.

NIPRNET – Non-classified Internet Protocol Router Network. The unclassified network of the US Department of Defense which provides Internet access as well as interconnectivity to DoD users and facilities.

NTLM - A Microsoft authentication protocol that uses cryptographic hash representations of account passwords. (See: http://msdn.microsoft.com/en-us/library/aa378749(VS.85).aspx)

PDF – File format and filename extension for Adobe Portable Document Format documents.

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.

RAR or Roshal Archive - A compressed file format similar in use to the more popular ZIP format. It is used to conserve storage and network resources and simplifies the movement of large sets of files. Optional encryption is available using the NIST Advanced Encryption Standard algorithm. Just as ZIP archives are created with software such as WinZip (http://www.winzip.com) and zip (http://www.info-zip.org), RAR archives are created with WinRar and RAR (http://www.rarlab.com)

Remote Desktop Protocol (RDP) - The communication protocol used to provide remote viewing and control of Microsoft Windows computers and applications. For additional information (See http://msdn.microsoft.com/en-us/library/aa383015(VS.85).aspx).

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.us-cert.gov/cas/tips/ST06-001.html).

Security Event and Information Management (SEIM) – Centralized collection and management of security event records from many different systems such as firewalls, IDS/IPS, antivirus software, authentication systems, etc. SEIMs may provide complex multifactor rules to alert on patterns of behavior not easily identifiable by one of the component systems alone.

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.

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).

Tunneling - A technique to encapsulate one communication data stream inside of another, in order to extend the advantages of the latter to the former. Attackers will often tunnel a network protocol that would not be allowed to cross network boundaries inside of another that is allowed, defeating perimeter defenses (See: http://www.its.bldrdoc.gov/projects/devglossary/_tunneling.html).

Two-factor Authentication (T-FA) - Existing authentication methodologies involve three basic "factors":

- Something the user knows (e.g., password, PIN);
- Something the user has (e.g., ATM card, smart card); and
- Something the user is (e.g., biometric characteristic, such as a fingerprint).

T-FA requires that a user present two of the three possible factors to the authentication mechanism. A known flaw in some T-FA systems is the server storage of a hash representation of the credentials contained on the smart card or token. With this in hand, the attacker can replay that data to the authentication system; in this case, that of the proxy server, without needing the physical card or token (See: http://www.ffiec.gov/pdf/authentication_guidance.pdf).

USPACOM – 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.

USTRANSCOM - United States Transportation Command provides intermodal transportation across the spectrum of military operations. USTRANSCOM 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.

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

Anderson, Robert H, Feldman, Phillip M., et al., *Securing the U.S. Defense Information Infrastructure*, RAND Corp., 1999.

Aning, Jerome and Olchondra, Riza T., RP Gov't Websites Vulnerable to Hacking, *Philippine Daily Inquirer*, March 31, 2009, http://technology.inquirer.net/infotech/infotech/view/20090331-197122/RP-govt-websites-vulnerable-to-hacking#

Asian News International, "French Embassy Website in China Hacked," *ZeeNews*, December 12, 2008, http://www.zeenews.com/news490316.html

AsiaPulse News, "China-Based Hackers Access S. Korean Finance Ministry's Intranet," April 8, 2009, http://www.highbeam.com/doc/1G1-197405142.html

Ball, Desmond, "Signals Intelligence in China" *Jane's Intelligence Review*, August 1, 1995.

Blasko, Dennis J., *The Chinese Army Today*, Routledge, 2006.

Bliss, Jeff, ''China's Spying Overwhelms U.S. Counterintelligence,'' *Bloomberg,* April 2, 2007, http://www.bloomberg.com/apps/news?pid=20601087&sid=ab2PiDl1qW9Q&refer=home

Bristow, Damon, "Cyber-warfare rages across Taiwan Strait," *Jane's Intelligence Review*, Vol 12, Issue 2, February 1, 2000.

Cheng, Dean, "PLA Views on Space: The Prerequisite for Information Dominance," Center for Naval Analysis, CME D0016978.A1, October 2007

Christensen, Thomas J., "Windows and War: Trend Analysis and Beijing's Use of Force," in *New Directions in the Study of China's Foreign Policy*, Alastair Iain Johnston and Robert Ross, eds. Stanford University Press, 2006.

Cui Yafeng, "On Changes in Relationship Strategy Has With Campaigns and Battles in Modern Warfare", *China Military Science*, December 29, 2008, Translated by OSC, CPP20081229563002.

Dai Qingmin, "On Seizing Information Supremacy," *China Military Science*, April 20, 2003, No 2, Vol. 16, pp 9-17, Translated by OSC, CPP20020624000214.

—"On Integrating Network Warfare and Electronic Warfare," *China Military Science,* February 1, 2002, pp 112-117, Translated by OSC, CPP20021062400024.

Blakely, Rhys, Richard, Jonathan, Rossiter, James and Beeston, Richard, "MI5 Alert on China's Cyberspace Spy Threat," *The Times*, December 1, 2007, http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece

Chickowski, Ericka, "Naval War College Network Shuts Down After Chinese Attack," *SC Magazine*, December 9, 2006, http://www.scmagazineus.com/Naval-War-College-network-shuts-down-after-Chinese-attack/article/34305/

Elegant, Simon, "Enemies at the Firewall," *Time Magazine,* December 6, 2007, http://www.time.com/time/magazine/article/0,9171,1692063,00.html

Epstein, Keith and Elgin, Ben, *Network Security Breaches Plague NASA*, Business Week, November 20, 2008. http://www.businessweek.com/magazine/content/08_48/b4110072404167.htm

Fan Li , "Exploration of Construction of Security Defense Architecture for Military Information System;" *Computer Security*, February 1, 2009 pp 90, Translated by OSC, CPP20090528670007.

Faiola, Anthony, "Cyber Warfare: China vs. Japan," *MSNBC News*, May 11, 2005, http://www.msnbc.msn.com/id/7796346/

Ferster, Warren and Clark, Colin, "NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft," by, *Space News Business Report*, October 3, 2006, http://www.space.com/spacenews/archive06/chinalaser_1002.html

Fisher, Richard Jr., "People's Liberation Army Leverage of Foreign Military Technology," March 22, 2006, International Assessment and Strategy Center, http://www.strategycenter.net/research/pubID.97/pub_detail.asp.

Gartzke, Ulf, "Outrage in Berlin Over Chinese Cyber Attacks," *The Weekly Standard*, August 31, 2007,

http://www.weeklystandard.com/weblogs/TWSFP/2007/08/outrage_in_berlin_over_chinese.asp

Goetz, John and Rosenbach, Marcel, "Cyber Spies: 'GhostNet' and the New World of Espionage," *Der Speigel Online*, April 10, 2009, http://www.spiegel.de/international/world/0,1518,618478,00.html

Gong Gucheng, "Information Attack and Information Defense in Joint Campaigns," *Military Art Journal*, October 1, 2003, Translated by OSC, CPP20080314623007.

Grow, Brian, Epstein, Keith, Chi-Chu Tschang, "The New E-spionage Threat," *BusinessWeek*, April 10, 2008, http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

Harris, Shane, "China's Cyber-Militia," *The National Journal*, May 31, 2008, http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php

Henderson, Scott, *The Dark Visitor*, January 2007.

Hess, Pamela, "China Prevented Repeat Cyber Attack on US," *UPI*, October 29, 2002. http://www.upi.com/Business_News/Security-Industry/2002/10/29/China-prevented-repeat-cyber-attack-on-US/UPI-88751035913207/

Homeland Security Newswire, *China Suspected in Hacking Attempt on Oak Ridge National Lab*, December 10, 2007; http://homelandsecuritynewswire.com/single.php?id=5198

Singh, Gurmukh, "Chinese Hack Into Indian Embassies, Steal Dalai Lama's Documents," *IANS*, March 2009, http://www.thaindian.com/newsportal/sci-tech/chinese-hack-into-indian-embassies-steal-dalai-lamas-documents_100172617.html

Information Office of the State Council of the People's Republic of China, *China's National Defense in 2004*,, Beijing, 27 December 2004. http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html

—*China's National Defense in 2006,* December 29, 2006, http://english.chinamil.com.cn/site2/news-channels/2006-12/29/content_691844.htm

—*China's National Defense in 2008*, January 20, 2009, http://www.chinadaily.com.cn/china/2009-01/20/content_74133294.htm

Jane's Sentinel Security Assessment, "China and Northeast Asia," April 3, 2009.

Johnston, Alastair Iain, "China's Militarized Interstate Dispute Behavior 1949-1992: A First Cut at the Data," *The China Quarterly*, 1998, No.153 (March 1998).

Kamphausen, Roy and Scobell, Andrew, eds., *Right Sizing The People's Liberation Army: Exploring The Contours Of China's Military,* Strategic Studies Institute, September 2007.

K'an Chung-kuo, "Intelligence Agencies Exist in Great Numbers, Spies Are Present Everywhere; China's Major Intelligence Departments Fully Exposed, *Chien Shao*, No 179, January 1, 2006, Translated by OSC, CPP20060110510011.

Ke Zhansan, "Studies in Guiding Ideology of Information Operations in Joint Campaigns," *China Military Science,* April 20, 2003, Translated by OSC, CPP2003728000210.

Lague, David, "Chinese See Military Dependence on Computers as Weakness," *The New York Times*, August 29, 2007, http://www.nytimes.com/2007/08/29/world/asia/29iht-cyber.1.7299952.html

Liao Wenzhong, "China Military Net Force: National Security, Public Security, and the People's Liberation Army," *Ch'uan-Ch'iu Fang-Wei Tsa-Chih* , March 2007, Translated by OSC, CPP20071023318001.

Li Deyi, "A Study of the Basic Characteristics of the Modes of Thinking in Informatized Warfare," *China Military Science*, August 20, 2007, pp 101-105, Translated by OSC, CPP20081028682007.

Li Zhilin, "On the Trend of Changes in Operations Theory Under Informatized Conditions," November 12, 2008, Translated by OSC, CPP20081112563002.

Lu Qiang, "*Zhuoyan Xinxihua Zhanzheng Tedian Jiaqiang Chengshi Minbing Jianshe,"* (Focus On The Characteristics Of Information Warfare To Strengthen The City Militia Construction), *China Militia Magazine*, August 2003, http://www.chinamil.com.cn/item/zgmb/200308/txt/16.htm

Marquand, Robert and Arnoldy, Ben, "China Emerges as Leader in Cyberwarfare," *The Christian Science Monitor*, September 14, 2007, http://www.csmonitor.com/2007/0914/p01s01-woap.html

McMillan, Robert, *US Defense Department Under Cyber Attack*, IDG News Service, June 2007.

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

Melvin, Ellis L., *A Study of The Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureau*, June 19, 2005.

"Minbing Wangluo Zhan Fendui Zhize" (Duties of the Network Warfare Militia Unit), March 16, 2008. http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp?infoNo=26366

Minnick, Wendell, "Taiwan Faces Increasing Cyber Assaults," *Army Times Publishing*, June 12, 2006, http://minnickarticles.blogspot.com/2009/09/taiwan-faces-increasing-cyber-assaults.html

Moore, Malcolm, "China's Global Cyber-Espionage Network GhostNet Penetrates 103 Countries," Telegraph.co.uk, March 29, 2009, http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html

Mount, Mike, *Hackers Stole Data on Pentagon's Newest Fighter Jet*, CNN, April 21, 2009, http://www.cnn.com/2009/US/04/21/pentagon.hacked/index.html

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

Norton-Taylor, Richard, "Titan Rain – How Chinese Hackers Targeted Whitehall," *The Guardian*, September 5, 2007, http://www.guardian.co.uk/technology/2007/sep/04/news.internet

Onley, Dawn and Wait, Patience, "Red Storm Rising: DoD's Efforts to Stave Off Nationn-State Cyberattacks Begin with China," *Government Computer News*, August 17, 2006, http://www.gcn.com/Articles/2006/08/17/Red-storm-rising.aspx

Peake, Ross, "Australia Confirms Cyber Attacks, Canberra Times," August 3, 2008, http://www.canberratimes.com.au/news/local/news/general/australia-confirms-cyber-attacks/510016.aspx

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

Schwankert, Steven, "US Congressmen Accuse China of Hacking Their Computers," *IDGNS*, June 12, 2008, http://www.infoworld.com/archive/200806?page=46

Sevastopulo, Demetri, "Hackers Breach White House System," *The Financial Times,* November 6, 2008, http://us.ft.com/ftgateway/superpage.ft?news_id=fto11062008193836072 6&page=2

Sevastopulo, Demetri, *Cyberattacks on McCain and Obama Team's 'Came from China'*, The Financial Times, November 6, 2008.

Shi Zhihua, Basic Understanding of Command of Information Operation," *China Military Science*, No. 4, 2008, Translated by OSC, CPP20090127563002.

The Straits Times, "Chinese Plan to Hack into Taiwan Websites," October 10, 2000, http://www.hartford-hwp.com/archives/55/105.html

Stokes, Mark A, *China's Strategic Modernization: Implications for the United States,* U.S. Army Strategic Studies Institute, September, 1999.

Tamura, Hideao and Soma, Masaru, "Japan Increasingly 'Susceptible to Cyber Attacks from Chinese PLA," *Tokyo Sankei Shimbun*, October 2007.

Tang, Rose, "China Warns of Massive Hack Attacks," *CNN*, May 3, 2001, http://archives.cnn.com/2001/WORLD/asiapcf/east/05/03/china.hack/

Thornburgh, Nathan, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them," Time Magazine, August 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098961,00.html

Tung, Liam, "China Accused of Cyberattacks on New Zealand," CNET News, September 13, 2007, http://news.cnet.com/China-accused-of-cyberattacks-on-New-Zealand/2100-7348_3-6207678.html

US China Economic and Security Review Commission, *2007 Report to Congress,* November 2007, http://www.uscc.gov

US Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2006*, May 2006.

—*Annual Report to Congress: Military Power of the People's Republic of China 2009,* March 2009.

—*Joint Publication 4-0: Joint Logistics,* 18 July 2008, http://www.dtic.mil/doctrine/jel/new_pubs/jp4_0.pdf

US Pacific Command, Virtual Information Center, "People's Republic of China Primer," August 4, 2006, http://www1.apan-info.net/Portals/45/VIC_Products/2006/08/060804-P-China.doc

Wang Houqing, Zhang Xingye, Huang Bin, and Zhan Xuexi, eds*, The Science of Campaigns*, National Defense University Publishing House, May 2000, Translated by OSC, in CPP20010125000044.

Whiting, Allen S., "China's Use of Force 1960-1996, and Taiwan," *International Security*, Vol. 26, No. 2, Fall, 2001.

Ye Youcai and Zhou Wenrui, "Building a High-quality Militia Information Technology Element" *National Defense*, September 15, 2003 pp 45, Translated by OSC, CPP20031002000138.

"Yongning is the First to Set Up Information Warfare Militia Units," March 19, 2008, http://old.chinayn.gov.cn/info_www/news/detailnewsb.asp

Zhu Jianjian and Li Lijian, "Memorandum on National Defense Reform and Innovation (Part 5): Website Established by Ezhou Militia," *National Defense,* May 2001, Translated by OSC CPP20090102670001.