

SECTION 4: CHINA'S CYBER ACTIVITIES THAT TARGET THE UNITED STATES, AND THE RESULTING IMPACTS ON U.S. NATIONAL SECURITY

“The Commission shall investigate and report exclusively on—

...

“REGIONAL ECONOMIC AND SECURITY IMPACTS—The triangular economic and security relationship among the United States, Taipei and the People’s Republic of China (including the military modernization and force deployments of the People’s Republic of China aimed at Taipei), the national budget of the People’s Republic of China, and the fiscal strength of the People’s Republic of China in relation to internal instability in the People’s Republic of China and the likelihood of the externalization of problems arising from such internal instability. ...”

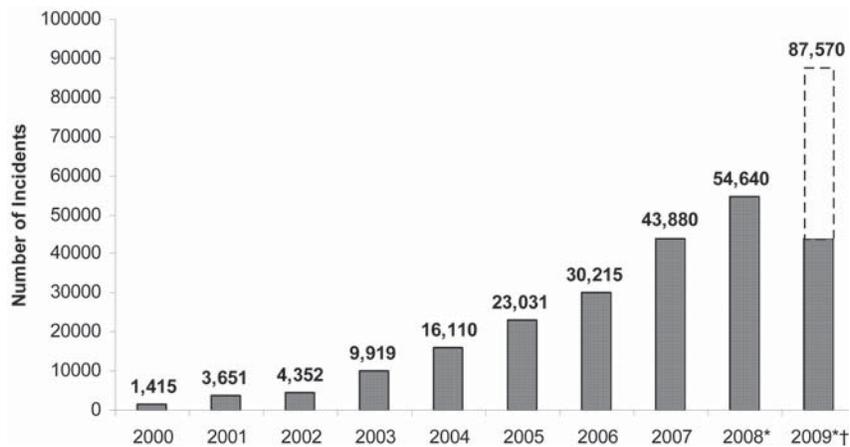
Introduction

In May 2009, President Obama labeled cyber attacks “one of the most serious economic and national security challenges” that the country faces.³⁴⁵ Joel Brenner, former director of the Office of the National Counterintelligence Executive, has identified China as the origin point of extensive malicious cyber activities that target the United States.³⁴⁶ Anecdotal evidence suggests that Chinese attacks targeting U.S. government- and defense-related information have been damaging. For example, in June 2007, the Office of the Secretary of Defense took its information systems offline for more than a week to defend against a serious infiltration that investigators attributed to China.³⁴⁷ In April 2009, reports surfaced that attacks on defense contractor information systems in 2007 and 2008 allowed intruders—probably operating from China—to successfully exfiltrate “several terabytes of data related to design and electronics systems” of the F35 Lightning II, one of the United States’ most advanced fighter planes.³⁴⁸ A large body of both circumstantial and forensic evidence strongly indicates Chinese state involvement in such activities, whether through the direct actions of state entities or through the actions of third-party groups sponsored by the state.

Malicious cyber activity has the potential to destroy critical infrastructure, disrupt commerce and banking systems, and compromise sensitive defense and military data. Malicious cyber incidents are on the rise, and attacks against U.S. government computer systems illustrate the severity of the problem. In testimony to the Commis-

sion in May 2008, Colonel Gary McAlum, then chief of staff for the U.S. Strategic Command's Joint Task Force for Global Network Operations, stated that the reported incidents of malicious cyber activity against the Department of Defense reached 43,880 throughout 2007.³⁴⁹ For 2008, that figure increased almost 20 percent, to 54,640 incidents. The numbers from the first half of 2009 foretell a steep increase for this year as well: 43,785 incidents occurred from January 1 to June 30.³⁵⁰ If these trends continue through the end of 2009, there would be a 60 percent increase in malicious cyber activity compared to 2008. The cost of such attacks is significant. Army Brigadier General John Davis, deputy commander of the Joint Task Force-Global Network Operations, stated in April 2009 that, in just the preceding six months, the U.S. military alone had spent more than \$100 million on "manpower, time, contractors, tools, technology and procedures" to remediate attacks on its networks.³⁵¹

Figure 1: DoD Reported Incidents of Malicious Cyber Activity, 2000–2008, With Projection for 2009



Source: U.S.-China Economic and Security Review Commission, *Hearing on China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities*, testimony of Gary McAlum, May 20, 2008.

*Source: Name withheld (staff member, U.S. Strategic Command), telephone interview with Commission staff, August 28, 2009.

†Solid portion accounts for reported malicious incidents from January 1 to June 30, 2009, as provided by the U.S. Strategic Command. Dotted portion estimates malicious incidents from July 1 to December 31, 2009, assuming a constant rate of attacks throughout the year.

In 2009, the executive branch of the U.S. government took several measures in order to address cyber threats to national security. In April, the White House announced the creation of a position called the "Cyber Security Coordinator" (known colloquially as the "Cyber Czar"), who will manage a more centralized and "top-down" approach to the U.S. government's interagency cybersecurity process and make recommendations for the nation's cyber policies and standards.³⁵² The coordinator will have some budgetary control over new and existing initiatives through the Office of Management and Budget,³⁵³ and he or she would report to both the National Se-

curity Council and the National Economic Council.³⁵⁴ In June 2009, Secretary of Defense Robert Gates directed the Department of Defense to form a unified Cyber Command in order to “develop a comprehensive approach to [Department of Defense] cyberspace operations.”³⁵⁵ The new command, which will include the National Security Agency and at least initially be subordinate to the U.S. Strategic Command, reportedly will integrate the Department of Defense’s offensive and defensive cyber capabilities. The extent to which the Cyber Command will work to secure nondefense or intelligence-related government networks and civilian network infrastructure remains unclear; the Department of Homeland Security may retain the majority of that responsibility.³⁵⁶

Attribution of Responsibility for Cyber Attacks

Cyber attacks that originate in China can defy easy classification; some malicious activity appears to originate from private hacking groups, while other activity is almost certainly state sponsored. The latter, which will be the primary focus of this section, can be recognized to a certain extent by two important factors. First, cyber incidents leave behind signatures that can, with forensic analysis, sometimes reveal the affiliation of the responsible actors to a reasonable degree of certainty. This sometimes allows investigators to implicate the Chinese government directly, or sometimes even specific parts of the Chinese government, such as the People’s Liberation Army (PLA).³⁵⁷ Although this section draws on the conclusions of investigators involved in conducting forensic analysis of cyber intrusions, a thorough description of the techniques used is not publicly available.

Second, the nature of the malicious activity—including the type of information targeted—helps supplement the understanding of the attackers and their affiliations. One can infer state involvement in some instances based on the specific targeting of government and defense networks. According to a study for the Commission by Northrop Grumman that implicates the Chinese government in extensive malicious cyber activities against the United States,

*China is likely using its maturing computer network exploitation capability to support intelligence collection against the U.S. government and U.S. defense industries by conducting a long-term, sophisticated, computer network exploitation campaign. . . . 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.*³⁵⁸

On whether attackers are in the employ of the Chinese government or just selling information the attackers have stolen after the fact, the study suggests that “[i]f 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.”³⁵⁹

Department of Defense Definitions for Cyber Activity

This section uses the following definitions to describe the tactics used in cyber activities:

Computer Network Operations: “Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.”³⁶⁰

Computer Network Exploitation: “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.”³⁶¹

Computer Network Attack: “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.”³⁶²

Computer Network Defense: “Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.”³⁶³

The Development of Doctrine in China for Computer Network Operations

The Chinese government’s lack of transparency in the field of computer network operations makes analysis of the involvement of Chinese state actors challenging at the unclassified level. However, while much about China’s government-backed computer network warfare programs remains opaque, military newspapers and professional military journals in China have long expressed professional admiration for perceived U.S. network and electronic warfare capabilities in conflicts such as the 1999 Kosovo campaign and the 2003 invasion of Iraq and have discussed the need to catch up.³⁶⁴ These journals have engaged in a surprisingly open discussion of the need to develop greater capabilities for computer network operations and have even provided a number of details as to what form these capabilities should assume.³⁶⁵

The Chinese government has not publicly issued a strategy or governing concepts for computer network operations³⁶⁶ such as those contained within *Joint Publication 3-13: Information Operations*, released in 2006 by the U.S. Department of Defense.³⁶⁷ However, some determined western open-source researchers have been able to gain insights into the institutional developments of China’s cyber capabilities through studying the debates in these journals.

Chinese Terms for Computer Network Operations

Researchers with the Center for Naval Analyses have identified and translated the major doctrinal terms employed by Chinese military authors as follows:³⁶⁸

“*Computer network warfare*”: equivalent meaning to the U.S. doctrinal term “computer network operations”;

“*Computer network attack*”: same as the U.S. doctrinal term “computer network attack”;

“*Computer network defense*”: same as the U.S. doctrinal term “computer network defense”;

“*Computer network reconnaissance*”: equivalent meaning to the U.S. doctrinal term “computer network exploitation.”

When the preceding terms are discussed in this chapter within a Chinese context, they will be used interchangeably with their U.S. counterparts.

Researchers such as Timothy Thomas of the Foreign Military Studies Institute at Fort Leavenworth, Kansas, have been able to assemble detailed histories of the development of PLA network warfare thought over the past decade.³⁶⁹ The PLA views computer network warfare as both a key enabler of modern warfare and a critical new spectrum of conflict in its own right. These professional journal writings describe actions against an enemy’s command, control, computers, communications, intelligence, surveillance, and reconnaissance nodes, and the defense of one’s own, as the critical foci of modern warfare—thereby raising even further the importance of computer network operations. Chinese analysts also describe computer network warfare as a critical tool that can be exploited by a weaker military force to level the playing field against a stronger opponent.³⁷⁰

“Integrated Network Electronic Warfare”

Analysis of writings from authoritative PLA publications also has revealed the existence of a guiding PLA operational concept titled “Integrated Network Electronic Warfare.” Integrated Network Electronic Warfare incorporates elements of computer network operations in tandem with elements of traditional electronic warfare.³⁷¹

Integrated Network Electronic Warfare advocates the employment of traditional electronic warfare operations—such as the jamming of radars and communications systems—in coordination with computer network attack operations. The goal is to create a multi-spectrum attack on enemy command, control, communications, computers, intelligence, surveillance, and reconnaissance systems in the early stages of conflict, thereby denying the opposing force access to information and communications necessary to move forces and fight in a modern battlespace.

As summarized in a 2009 publication, Integrated Network Electronic Warfare would use

techniques such as electronic jamming, electronic deception and suppression to disrupt information acquisition and in-

*formation 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.*³⁷²

While some aspects of Integrated Network Electronic Warfare may remain aspirational for the Chinese military, the PLA takes the concept seriously and views cyberspace, in tandem with the electromagnetic spectrum, as critical arenas of conflict in full spectrum modern warfare. (For further discussion of China's military modernization, see chap. 2, sec. 1, of this Report, "China's Military and Security Activities Abroad.") The 2007 revised Outline for Military Training and Evaluation training guidance issued by the PLA General Staff Department directed all branches of the PLA to make training "under complex electromagnetic environments" the core of campaign and tactical training.³⁷³

In one recent example of such training, in early January 2008 approximately 100 senior-ranking PLA officers from multiple service branches reportedly observed an Integrated Network Electronic Warfare exercise hosted by elements of a group army of the Shenyang Military Region. In the exercise, troops of the defending PLA forces had to fend off attacks from mock aggressor forces* employing simulated cyber and electronic attacks. These attacks included a computer virus that sowed confusion by changing logistics requirements, using electrical pulse attacks that destroyed computer motherboards, and jamming communications and radar systems.³⁷⁴

Chinese Government Entities Involved in Computer Network Operations

The Third and Fourth Departments of the PLA General Staff Department

The Third Department of the PLA General Staff Department, which has traditionally engaged in signals intelligence collection, bears primary responsibility within the PLA for computer network exploitation. For these purposes, the organization likely maintains "technical reconnaissance bureaus" within each of China's seven military regions. The Fourth Department of the PLA General Staff Department, which has traditionally engaged in electronic warfare, plays the leading role in computer network attack.³⁷⁵

In 2009, the Commission contracted with the Northrop Grumman Corporation to perform a detailed, unclassified study on the development of Chinese capabilities for conducting cyber warfare and cyber espionage. This report, titled "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," contains significant additional detail on PLA entities involved in cyber warfare. The full report is now available on the Commission's Web site.³⁷⁶

*In U.S. military exercises, the friendly (i.e., U.S.) forces are identified as "blue," and the opposing aggressor forces are "red" forces. In PLA exercises, this convention is reversed: The Chinese forces are "red," and the units acting the role of the enemy are the "blue" forces.

The Role of “Information Warfare Militia” Units of the PLA

The efforts of the PLA regarding computer network warfare are not limited solely to its active duty forces. The PLA has been forming cyber militia units since the late 1990s, “comprised of personnel from the commercial information technology sector and academia ... represent[ing] an operational nexus between PLA [computer network operations] and Chinese civilian information security professionals.”³⁷⁷ The first such unit formed may be one created on an experimental basis in Datong City, Shanxi Province, in early 1998.³⁷⁸ According to Chinese press reports, at the time of its creation the Datong unit contained 40 personnel³⁷⁹ and was located within “a certain Datong City state-owned enterprise.”³⁸⁰ The unit relies upon “the resources of the local area’s scientific talent, information technology, and facilities,” with personnel drawn from “all over the city’s 20 scientific research institutes, universities, and information occupations.”³⁸¹ In 2006, the authoritative Chinese Academy of Military Science published an article that explicitly endorsed the information warfare militia concept and directed the PLA to make the creation of such units a priority.³⁸²

A 2008 study by the Internet security research firm iDefense identified 33 probable such militia units, mostly located within government research institutes, information technology firms, or university computer science departments. Personnel recruited for these units tend to be young (under 45 years of age); many are professors or graduate students and/or have experience with information technology gained through work with civilian information technology firms and may also have foreign language skills useful for intelligence collection.³⁸³ PLA commanders reportedly have been directed to relax standard age and physical fitness requirements for the members of information warfare militia units in order to ensure that individuals with valuable skills not be turned away or attrited from the ranks.³⁸⁴

Other sources indicate that political reliability is also a factor in the selection of personnel: An article from an authoritative military journal about the process of forming a particular information warfare militia unit described the importance of a “thorough analysis of the degree of ideological awareness” of each recruit and further indicated that 94 percent of the selected personnel were members either of the Chinese Communist Party or its Communist Youth League.³⁸⁵

A Profile of a Chinese Information Warfare Militia Unit

In March 2008, the PLA established an information warfare militia unit in Yongning County, in Ningxia Province. The establishment ceremony for the unit was publicized by the local government and included a number of prominent local figures, including the local PLA garrison commander and chief of staff as well as leading officials of the county government.³⁸⁶

According to a concurrent Web posting made by the county government, the duties of an information warfare militia unit include “[s]trengthening research and exercises related to network warfare, and continuously improving methods for network attacks. . . . In peacetime, extensively collect information from adversary networks and establish databases of adversary network data. . . . In wartime, attack adversary network systems, and resist enemy network attacks.”³⁸⁷

According to a press release about the establishment ceremony for the unit, the Yongning Militia Information Warfare Unit will have approximately 80 personnel divided into three detachments, focused on network warfare, information collection and processing, and network defense. The unit was constructed according to “standardized requirements,” with facilities including an operations center, a generator room, the commander’s office, an activities room, and a set of charts and other necessary materials.

The same source indicated that individual unit personnel would undergo 10 days of foundational military training, including basic military skills and general knowledge of network warfare. A “Three-Year Development Plan” for the training of the unit was also mentioned, but no further details were provided. Finally, the local government announcement also underscored concern for the loyalty and political reliability of unit members, stating that their efforts would build “a unit that is steadfast in political belief, that has pure ideology and morals, that has a superior quality of professionalism . . . that performs propaganda for the Party, that benefits the people, and that can provide effective strength to the military for winning future wars under informationized conditions.”³⁸⁸

The Role of “Patriotic Hackers”

Another category of actors involved in cyber activities directed against the United States consists of privately organized groups of Chinese computer hackers, sometimes referred to as “patriotic hackers” or “red hackers.”³⁸⁹ Motivated both by a desire to test their hacking skills as well as an antiwestern sense of Chinese nationalism, such groups have been involved in many high-profile “hacktivist” defacements or distributed denial of service attacks directed against U.S. Web sites. These have most frequently occurred during times of strained Sino-American relations, such as in the aftermath of the accidental May 1999 bombing of a People’s Republic of China (PRC) embassy annex in Serbia by U.S. forces, or following the April 2001 collision between a U.S. Navy EP-3 surveil-

lance aircraft and a PLA Navy F-8 fighter aircraft over the South China Sea.³⁹⁰ Many Chinese hacker organizations operate quite openly on the Internet, maintaining their own Web pages, recruiting new members, and boasting of their hacking exploits. In the past, these groups have generally been tolerated by the Chinese government, as long as their hacking activities were directed abroad.³⁹¹

It remains unclear as to the extent these “red hackers” receive support or sanction from the Chinese government. Some experts on Chinese hacker groups have tended to emphasize that they are indeed privately organized and that they operate largely independent of the government.³⁹² These arguments also emphasize that, from the point of view of the PRC authorities, “several factors argue against formal PLA plans to include ‘hacktivism’ as part of a [computer network operations] campaign.”³⁹³ One such factor could be concerns about reliance upon personalities assessed to be unsuited for disciplined government service,³⁹⁴ a concern that may be further revealed in the strong emphasis placed on political reliability in the selection of personnel for information warfare militia units (see above). Other factors could include the unpredictable nature of red hacker activity in the midst of a crisis in which the government might wish to control both escalatory measures and international public opinion,³⁹⁵ as well as the need to control the list of targets selected for computer exploitation or attack.³⁹⁶ The Chinese government has recently signaled its intent to rein in privately initiated, unsanctioned hacker activity, publishing antihacker editorials in the state media,³⁹⁷ passing the February 2009 antihacking law by the National People’s Congress,³⁹⁸ and arresting members of some hacker groups.³⁹⁹

However, these factors aside, there are clear signs of relationships between Chinese government agencies and some individual hackers or red hacker groups. Reservations that might apply to a wartime computer network operations campaign do not necessarily apply to peacetime computer exploitation and cyber harassment, and the PRC appears willing to make use of its “patriotic hackers” for certain of these tasks.⁴⁰⁰ For example, the Chinese government has encouraged efforts to counter “foreign forces subverting China via the Internet,” and red hackers have duly directed distributed denial of service attacks, malicious code, and computer exploitation activity against the Web sites and affiliated users of pro-Tibet, pro-Xinjiang, Falun Gong, and Chinese prodemocracy organizations.⁴⁰¹ Additionally, at least one prominent Chinese hacker is known to have been recruited into the ranks of an information warfare militia unit,⁴⁰² and in 2007–2008 the Ministry of Public Security (one of China’s primary domestic security agencies) placed job recruitment postings on *EvilOctal.com* and *XFocus.net*, two of China’s foremost hacker forum Web sites.⁴⁰³

These latter examples may be part of a broader recent trend—the Chinese government’s effort to draw from the talent available in its hacker community while also curbing some freelance hacker activities and seeking to bring them under state control. One aspect of this activity is the conversion of formerly state-tolerated, private hacker groups into information security firms that maintain extensive government ties and contracts.⁴⁰⁴ The PRC authori-

ties also have made high-profile arrests of selected hackers, intended to send a clear message that their activities could come under state supervision if they were to continue. One such example was seen in Henan Province in February 2006, when

*[the] authorities shut down The Patriot Hackers—Black Eagle Base Website and arrested its members. ... The group, however, was operational again six months later. ... At that time its members released a statement that the group vowed to focus its efforts on training people for the state and working to improve the state's security network. ... The Black Eagle leadership also expressed appreciation to the State Security Bureau ... for the educational guidance they provided to members while in custody.*⁴⁰⁵

Profiles of Alleged Chinese Cyber Espionage

Cases of cyber espionage that leave trails leading back to China are observable across the spectra of business, politics, and technological research. These include instances of computer exploitation directed against Chinese ethnic and political dissident groups abroad, Members and offices of the U.S. Congress, and U.S. infrastructure targets. An examination of the particulars of these cases highlights the extensive and persistent character of probable state-sponsored Chinese computer exploitation activity, as well as the serious potential threat that this activity poses to U.S. interests.

The “GhostNet”

In March 2009, researchers of the Information Warfare Monitor—a collaborative initiative of the The SecDev Group, a think tank based in Ottawa, Canada, and the Citizen Lab, an interdisciplinary information technology and social science research institute based at the University of Toronto⁴⁰⁶—released a highly detailed report on their research into a wide-ranging cyber espionage network. Their forensic investigation revealed that the network, which they came to call “GhostNet,” had infected 1,295 host computers in 103 different countries around the world, many of them belonging to embassies, ministries of foreign affairs, and other high-profile government targets.⁴⁰⁷ While Information Warfare Monitor could not conclusively identify GhostNet’s operators, the circumstantial evidence surrounding GhostNet’s pattern of activity strongly suggested Chinese state involvement.

The Information Warfare Monitor forensic investigation started in the summer and autumn of 2008 with examinations of computers used by the personal office of the Dalai Lama; the Tibetan government-in-exile in Dharamsala, India; and Tibetan government-in-exile offices in New York, Brussels, and London. The researchers found multiple computers that had been infected with malicious software (malware) implanted by e-mails masquerading as legitimate messages sent either by professional contacts or by persons politically sympathetic to the intended victim. The e-mails contained either attached documents or Internet links that, when activated, installed malware. This malware would later connect to an external control server and download additional malware, including a remote administration tool (RAT) titled “gh0st RAT.”

“gh0st RAT” is a Trojan horse* that allows an attacker to remotely take full, real-time control of the computer. Once gh0st RAT was installed, the attacker could exfiltrate files, log keystrokes, and activate Webcams, among many other functions, all without the knowledge of the computer’s legitimate operator.⁴⁰⁸

By intentionally infecting a computer with the GhostNet malware, the Information Warfare Monitor researchers were able to observe the network’s activities and thereby identify the external servers issuing instructions to infected computers. They identified 26 “command” and “control” servers for GhostNet, all of which were located in China.⁴⁰⁹ The team also found that the control interface to the GhostNet network used the Chinese language.⁴¹⁰

The report also provides at least one concrete example that directly links Chinese intelligence officials to Internet monitoring of Tibetan exile groups. It describes the case of a young woman who had worked for two years in Dharamsala for a Tibetan nongovernmental organization named “Drewla,” an online outreach initiative founded in 2005 that uses Tibetans with Chinese language skills to engage young Chinese in online discussions.⁴¹¹ When attempting to enter Tibet from Nepal to visit her family, she was arrested and detained for two months. During this time, she was interrogated by PRC intelligence officials, who presented her with transcripts of her Internet chats. She was warned that her group was under surveillance and that its members were not welcome to return to Tibet.⁴¹²

The report is cautious in ascribing responsibility for GhostNet and warns against a “rush to judgment in spite of circumstantial and other evidence.” In its conclusion, however, the report does state that

*[the explanation] in which the circumstantial evidence tilts the strongest, would be that this set of high profile targets has been exploited by the Chinese state for military and strategic-intelligence purposes ... many of the high confidence, high-value targets that we identified are clearly linked to Chinese foreign and defence policy, particularly in South and South East Asia. Like radar sweeping around the southern border of China, there is an arc of infected nodes from India, Bhutan, Bangladesh and Vietnam, through Laos, Brunei, Philippines, Hong Kong, and Taiwan. Many of the high profile targets reflect some of China’s most vexing foreign and security policy issues, including Tibet and Taiwan.*⁴¹³

One of the authors of the GhostNet report, Rafal A. Rohozinski, principal and chief executive officer of The SecDev Group and advisory board member of the Citizen Lab at the University of Toronto, testified before the Commission in April 2009 and assented to a follow-on interview with Commission staff in September 2009. Mr. Rohozinski was cautious in ascribing GhostNet’s activity to the

* A “Trojan horse” is 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.” See Rita C. Summers, *Secure Computing Threats and Safeguards* (New York: McGraw-Hill, 1997), quoted in CERT, “Advisory CA-1999-02 Trojan Horses” (Pittsburgh, PA: Carnegie Mellon University, February 5, 1999). <http://www.cert.org/advisories/CA-1999-02.html>.

Chinese government but stated that “all the circumstantial evidence does point to a network which, in effect, is Chinese operated.” He also indicated that, based on analysis of Internet Protocol addresses, the team believed with “a high degree of confidence that the attackers were located in Hainan Island in China.”⁴¹⁴

Mr. Rohozinski also identified characteristics of GhostNet that indicated state sponsorship rather than the work of cyber criminals. He noted that the network was directed toward the collection of political intelligence rather than financial or personal data of interest to cyber criminals and that the particular targets—such as Tibetan exile groups and government ministries—were unlikely targets for profitable financial fraud.⁴¹⁵ He also noted that while the collection methods of GhostNet were relatively low-tech,

*[t]he requirements that would be needed to put in place to exploit the information gathered through [GhostNet] do require a scale larger than a small [nongovernmental organization]. Why? Linguistically, 103 different targets, including the Prime Minister’s Office of Laos, the Israeli Consulate in Hong Kong, the Russian Embassy in Beijing, the Iranian Foreign Ministry, requires linguistic skills as well as domain expertise in terms of being able to know what to look for and what to make of it.*⁴¹⁶

This analysis suggests that while the GhostNet’s methods for the collection of information were available to semiskilled private hackers, effective exploitation and analysis of that material probably required state resources. Mr. Rohozinski suggested that the intelligence collection of GhostNet likely represented state-sponsored activity carried out by private actors working on behalf of the government. As he stated,

[O]ur suspicion is that this was an operation which was essentially outsourced to third parties, essentially third-party actors possessing the equivalent of a letter of marque, legal pirates of the state, which had either some contractual arrangements or had some assurance of financial remuneration or reward in return for maintaining a specific kind of network such as this.

In support of this analysis, Mr. Rohozinski noted signs that GhostNet involved attackers from multiple vectors, with forensic analysis showing the affected computers to contain multiple infections of malware, “which means that it wasn’t just one GhostNet, it was a multiple of GhostNets.”⁴¹⁷ This analysis, which postulates private hacking groups undertaking intelligence collection under the sponsorship of the government, accords with the view of one of the leading western analysts of Chinese hacker organizations.⁴¹⁸ It also accords with activity discernible in human espionage and illegal technology acquisition conducted on behalf of the PRC, in which multiple private “entrepreneurial” actors are at work, and even in competition with one another, to procure information and technology on behalf of PRC institutions. (For more on this latter topic, see chap. 2, sec. 3, of this Report, “China’s Human Espionage Activities that Target the United States, and the Resulting Impacts on U.S. Security.”)

Case Study of Probable Chinese Network Intrusion Directed Against a U.S. Firm

The Northrop Grumman report prepared for the Commission provides a detailed case study about the 2007 penetration of an unnamed U.S. high-technology commercial firm's network. The penetration was carried out by hackers with probable ties to the Chinese government. A summary of this case study, below, describes the tradecraft commonly used in Chinese computer network operations.

In this instance, a first team of hackers, dubbed the "breach team," reconnoitered the firm's network for months. During this phase of the operation, the hackers gained critical information about computer accounts, employee names and passwords, and general network architecture. They mapped network directories to gain intimate knowledge of the contents of the compromised systems. The breach team then identified and exploited network vulnerabilities.

A second team of hackers, dubbed the "collection team," then used information gathered by the first team to collect sensitive information from the firm's network. Though linked to the first team through common attack vectors, the second team used different tools in unique ways, indicating distinct operators. The collection team quickly and efficiently navigated to precise directories and copied specific high-value files, often ignoring other similarly named and co-located files. This approach, given that the team opened none of the targeted files during the collection process, indicated precise knowledge of file contents as a result of the breach team's efforts and very specific tasking.

The collection team then copied the files and transferred them to high-speed "staging servers" within the firm's network. This decreased the attackers' operational footprint on machines known to the firm to contain high-value data, and it centralized activity on machines with high volumes of traffic, where the malicious activity would be more effectively disguised. The team then compressed and encrypted the files and assigned them innocuous names before exfiltrating the data from the firm's network.

The attackers demonstrated impressive professionalism and tradecraft. They discerned and attempted to secure only the most critical files. Throughout the process, the attackers consolidated attacks to one specific region—in the same time zone—in order to conduct activity after work hours in order better to avoid detection. The attackers set up redundant exfiltration channels so as to maximize the volume of data that they could simultaneously steal and to safeguard against errors and failures in the transfer process. Together, the teams accessed the firm's network on more than 150 occasions using dozens of legitimate but compromised accounts.

The attacks, at times, originated from a host with an Internet Protocol address located in China. The tools and techniques used in both the breach and collection phases of the attack were consistent with other attacks previously attributed to China. "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,” another factor that strongly indicates state or institutional sponsorship.⁴¹⁹

Instances of Probable Chinese Computer Network Exploitation and Attack Directed Toward Critical Infrastructure

In written testimony to the Commission, Kevin Coleman, senior fellow with The Technolytics Institute, an information security consultancy, warned of China’s computer exploitation activities and cited “reports of malicious code being found in the computer systems of oil and gas distributors, telecommunications companies, [and] financial services industries.” He highlighted the possibility of computer attacks on U.S. “water treatment and distribution systems.”⁴²⁰ These matters are of particular concern because, as the Department of Homeland Security’s 2009 National Infrastructure Protection Plan states, “[t]he United States relies on cyber infrastructure for government operations, a vibrant economy, and the health and safety of its citizens.”⁴²¹ All of these issues hinge to some extent on the operability of the U.S. electrical grid, which has surfaced as a prime target for attacks. This is perhaps because of the enabling role it plays with other types of infrastructure: communications, financial, and water networks all require electrical inputs.

Malicious actors use these probes to gain information for more deliberate exploitation. In April 2009, the *Wall Street Journal* reported pervasive penetration of the U.S. electric grid and other critical infrastructure nodes. According to the report, in some of these breaches intruders implanted software which, when remotely activated, could disrupt or destroy the system. Citing intelligence officials involved in the investigation, the *Wall Street Journal* report identified China as a primary actor in the intrusions.⁴²² The United States already may have suffered consequences from China’s exploitation of infrastructure controls. In May 2008, the *National Journal* reported that Chinese cyber attacks may have been responsible for blackouts in 2003 and 2007 in New York and Florida, respectively.⁴²³

Attacks on critical infrastructure could be used to gain an advantage in a time of crisis or war.⁴²⁴ Specifically seeking such targets is consistent with authoritative PLA writings on computer network operations. According to James Mulvenon, an expert in China’s cyber warfare practices, Chinese analysts state that “computer network attacks on nonmilitary targets are designed to ‘shake war resoluteness, destroy war potential and win the upper hand in war,’ thus undermining the political will of the population for participation in military conflict.”⁴²⁵

Instances of Probable Chinese Computer Network Exploitation Directed Toward the U.S. Congress

In December 2008, reports surfaced about the 2006 penetration of computers in the U.S. House of Representatives. Investigators found that the information systems of eight Congressmen and seven congressional committees had been compromised. After taking a roundabout route, the malware used in these attacks sought to establish connections to servers in China. While reports of the

attacks stopped short of directly linking them to the Chinese government, compelling circumstantial information suggests government ties. Aside from forensic data, for example, the lawmakers targeted had information with little or no intrinsic criminal value but immense political value. Among those attacked were Representative Frank Wolf (R-VA.), a Member with long-standing ties to human rights groups and prodemocracy activists, and Representative Mark Kirk (R-IL), then cochair of the U.S.-China Working Group, that, among other things, addresses bilateral trade issues.⁴²⁶

At least one Member of the Senate has also publicly complained of cyber intrusions into his office computer systems. On March 19, 2009 Senator Bill Nelson (D-FL) stated during a hearing of the Senate Armed Services Committee that “I have had my office computers invaded three times in the last month, and one of them we think is very serious.” An aide to Senator Nelson indicated that the attacks were traced to China through analysis of Internet Protocol data.⁴²⁷

Conclusions

- The quantity of malicious computer activities against the United States increased in 2008 and is rising sharply in 2009; much of this activity appears to originate in China.
- The direct attribution of such activities targeting the United States presents challenges due to hackers’ ability to conceal their locations. Nonetheless, a significant and increasing body of circumstantial and forensic evidence strongly indicates the involvement of Chinese state and state-supported entities.
- The Chinese government has institutionalized many of its capabilities for computer network operations within elements of the People’s Liberation Army. The PRC is also recruiting from its growing population of technically skilled people, including those from the private sector, to increase its cyber capabilities. It is recruiting skilled cyber operators from information technology firms and computer science programs into the ranks of numerous Information Warfare Militia units.
- China’s peacetime computer exploitation efforts are primarily focused on intelligence collection against U.S. targets and Chinese dissident groups abroad.
- In the early stages of a conflict, the PLA would employ computer network operations against opposition government and military information systems.
- Critical U.S. infrastructure is vulnerable to malicious cyber activity. Chinese military doctrine calls for exploiting these vulnerabilities in the case of a conflict.