What Lies behind Chinese Cyber Warfare

Gabi Siboni and Y. R.

兵之形，避實而擊虛
"Avoid strength, attack weakness."
Sun Tzu, *The Art of Warfare*

Introduction

Over the past several years China has been developing operational capabilities in the field of cyberspace warfare. A cyber attack may be defined as the unauthorized penetration of computer and communications systems belonging to individuals or organizations for the purpose of espionage and information theft, in order thereby to damage or disrupt the functioning of these systems or to damage other systems dependent on them, even to a point of causing actual physical damage. Despite denials by the Chinese government, researchers posit that China is behind a string of cyber attacks[1] against the United States,[2] Japan,[3] France,[4] Australia,[5] and other Western nations.[6]

Chinese activity in the field of cyberspace warfare is intensive and aggressive. It appears that China, focusing on extensive collection of intelligence and commercial information in various fields, is targeting a range of companies – from those with specific technological expertise to organizations with financial and economic knowledge, such as in the cyber attack on the International Monetary Fund in late 2011.[7] However, the fact that companies and organizations providing essential services and communications infrastructures have also been attacked suggests that

Dr. Gabi Siboni is a senior research associate and head of the Military and Strategic Affairs Program and Cyber Warfare Program at INSS. Y. R. is a senior figure at the Prime Minister's Office.

there many be other motives in play. If so, what underlies these attacks, and is it possible to identify the strategic principle with which China operates in the West in general and the United States in particular? To this end, one must examine China's cyber warfare strategy, the Chinese organizations involved in recent years, and the resources invested to realize China's goals through this type of warfare.

It is commonly assumed that before 2009, most of the attacks attributed to China were directed against the American military and the administration, such as Operation Titan Rain against American government agencies[8] and Operation Ghost Net against diplomatic targets in the UN. By contrast, in recent years the attacks attributed to China have been directed against civilian targets, including national infrastructures of critical importance, companies forming a part of the chain of access to those targets, and companies that if attacked, generate an outcome that serves an economic or commercial need.

In recent years there has also been a quantitative leap in attacks against infrastructures. The first was the Shady RAT series of attacks from mid-2006 until February 2011.[9] The second series was Operation Aurora, an especially sophisticated series targeting Google, a critical infrastructure at the global level. These started in mid-2009 and lasted until the end of that year. The third, which received a great deal of media attention, was against RSA, a company specializing in information security and internet servers providing secure ID and one-time password services.

This essay argues that an analysis of the publicly available information about the more recent attacks makes it possible to establish that China does in fact stand behind these attacks and also makes it possible to identify the link between China's cyberspace warfare strategy and its choice of targets. The analysis includes an examination of the companies attacked to identify possible motives for the attacks. For example, attacking companies and organizations supplying technology allows access to general cutting-edge technology, military technology, and so on. The motives for these attacks are presumably to steal capabilities and conduct industrial espionage against nations and commercial competitors. Attacking companies and organizations in the financial and even political sectors allows access to valuable intelligence in these fields. By contrast, the intelligence value for immediate use in attacking companies providing critical infrastructures and communications services is usually relatively low. Rather, gaining access, if only to some providers of communications and internet services in the West and the United States, is liable to give attackers the ability to damage these services.

China's Cyberspace Warfare Strategy

China's strategy of cyberspace warfare was formulated in the previous decade as part of a profound modernization process undertaken by the Chinese military. Based on the awareness that when it comes to kinetic warfare the Chinese armed forces are structurally inferior to the armed forces of the West, such as the United States military, the strategy reflects the understanding that in order to confront an enemy with technological superiority in the area of information flow, it is necessary to disrupt the enemy's access to this information. The approach involves dealing an opening blow comprising a cyber attack, an electronic attack, and a kinetic attack on the enemy's information web and military technology centers. Such a blow will lead to the creation of blind spots on the enemy's part, allowing Chinese forces to operate with greater efficiency.[10] The Chinese assumption is that by disrupting the flow of information it is possible to cause significant damage to the capabilities of a sophisticated enemy and gain an advantage in the early stages of a confrontation.

The strategy developed by China in the last decade sees integrated network operations[11] as a key platform for the field. The strategy is based on a combination of four types of operations:[12] attacks on computer networks; electronic warfare, including anti-electronic and anti-radar measures; computer network protection; and computer network exploitation.[13] One of the key components in the Chinese strategy is controlling the enemy's flow of information, on the operating assumption that China's enemies (especially Western nations, with an emphasis on the United States) are highly dependent on information flow-based technology. The assumption is that during a confrontation, the ability to damage the flow of information would allow China to attain an advantage in the physical battlefield. This integrated approach gives China interdisciplinary operational capabilities, allowing it to use force effectively to attack an enemy.

Selected publications have undertaken detailed analyses of the most important institutions in the Chinese military in terms of network operations.[14] This essay describes two of these central military bodies: the Third Bureau (in the General Staff of the People's Liberation Army), responsible for SIGINT, and the Fourth Bureau, responsible for ELINT and electronic warfare. The Third Bureau employs experts in many fields: technicians, computer experts, language experts, intelligence experts, and more. Indeed, several Western researchers have surmised that the manpower operating in the Third Bureau numbers over 130,000 personnel.[15] The vast scope of the bureau's activity and the range of missions with which it is charged make it eminently fit to carry out cyber operations on the web. This bureau has many "collection stations" throughout China; it is responsible for gathering intelligence from voice and related data, and fully processing and assessing it. The department is also apparently responsible for internal intelligence gathering in the Chinese military for the purpose of internal information security and protection. The Fourth Bureau, responsible for ELINT, i.e., electronic intelligence operations and electronic warfare, seems to operate also in the field of integrated network operations.[16] It appears that the Third Bureau is the body coordinating overall activity in this field.

In addition to the military organization, China also has a very large hacker community,[17] including hackers who have claimed responsibility for a number of cyber attacks and are apparently involved in operations driven by national goals. Although the Chinese government presumably takes steps to enforce Chinese law, which prohibits this type of activity, it often turns a blind eye to the phenomenon and even provides material support for some of it, in a type of outsourcing of government cyber activity.[18] In addition, the Chinese army recruits civilians – from the hacker community and hi-tech industry – to its web militia units.[19] The web militia is integrated with the regular military, though its members are unpaid volunteers.

In contrast to the common perception of Chinese cyber activities, some researchers claim that these activities are designed first and foremost for internal needs, and that Western nations need not be overly concerned about the threat to their cyberspace. In this view, the Chinese have developed capabilities primarily to monitor opponents to the regime and control information available to Chinese citizens, essentially for political needs largely directed at preserving the regime.[20] However, while totalitarian regimes, including China, indeed use cyberspace capabilities for internal political ends,[21] this is only part of the picture, as evidenced by the series of cyberspace incidents emanating from China in recent years.

One of the main components of China's cyberspace strategy is the critical need for access to enemy communications infrastructures; without this access it is difficult to plant powerful blind spots. Attaining effective access to communications networks requires extensive and long term work on infrastructures. An attack on enemy communications networks is possible only if there is regular access to them over time, providing attackers with high quality intelligence that allows them secretly to install malware for use when the time comes. Such access requires long term maintenance and preservation because of the constant changes enemies make in their communications and information set-ups, and because they continually install new defensive systems designed to uncover malicious activity.

China's Cyber Attacks

The last six years have seen more than a few cyberspace attacks attributed to China, which apparently were intelligence gathering operations. An analysis of these attacks affords a means to identify China's basic attack techniques and infer its policy and methods. The attacks portray a world power intent not on focusing on a specific target, rather on gaining wide infrastructure access. In the case of Operation Aurora, the goal was to gain access to Google's password mechanism and the versions control software. In the RSA attack, the goal was to gain access to the internal network in which all information relating to secure ID was managed; such access could in the future be used to mount a more effective attack on other companies using the system, including security companies and companies engaged in sensitive activity.

The techniques identified in the well organized attacks were highly similar, using social engineering,[22] exploiting software weaknesses, and inserting delay mechanisms to expand intra-organizational access and extract information. The fact that China has taken these measures in a consistent, systematic manner over the past several years strengthens the assertion that the attacks were designed deliberately and that the same organizations were responsible, and weakens the claim that the attacks were the work of random hackers. Further substantiation may be found in the analysis made by the Northrop Grumman Corporation,[23] which noted several criteria:

a. *Similarity in keyboard behavior*. Similar behavioral characteristics or patterns in the attackers' methods in the various attacks were identified, e.g., attacking similar information parts and using similar tools.
b. *Scope of preliminary preparations*. The attacks comprised actions requiring preparation and prior knowledge, stemming apparently from preliminary action taken over several months before the actual attack. For example, familiarity with the architecture of the attacked networks was clearly evident.
c. *Attacker discipline*. The attackers were highly disciplined, e.g., they did not open files to scan the contents initially before copying them, indicative of the probability that they were operating on the basis of prior information.

Operation Nitro

Operation Nitro involved a series of attacks that occurred primarily from late July 2009 until mid-September 2009, when Symantec published information about it.[24] Its main purpose, likely technological espionage, was carried out in several consecutive waves, distinguishable by their targets. At first, human rights organizations in China were attacked, followed by motor industries; in the final stage, 29 chemical companies were targeted. The targeted companies were Fortune 100 companies working in chemical R&D and special materials for application in military vehicles and companies involved in the construction of infrastructures for chemical industries and the manufacturing of advanced materials. The attack method was similar to the method used in other attacks launched by the Chinese and included the following components:

a. Malicious code usually disguised as a security update. A great deal of non-personalized email was sent to organizations, unlike other operations in which great efforts were made to direct the email to individual email addresses.
b. Insertion of a back door (Trojan horse) into the targeted computers.
c. Increased access to the networks attacked while using remnants of passwords found on the attacked computers in order to gain control of central network computers.
d. Collection of material on interim servers and dispatch of this material outside the network.

In all, some 100 computers were attacked, 29 in the chemicals field and 19 belonging to the security sector. Most of the companies attacked were in the United States (about 30 percent), Bangladesh (about 20 percent), and the United Kingdom (15 percent), with the remaining located in some 20 different states around the world.

Operation Aurora

Operation Aurora included a series of attacks beginning in mid 2009 and continuing until December of that year. In January 2010, Google was the first to report it. The company announced that the attackers had hacked into Gmail accounts belonging to Chinese dissidents active in the United States, Europe, and China.[25] Adobe also reported attacks in the same operation, which targeted at least 34 organizations and companies.[26] McAfee, the information security company, analyzed the attacks. The findings indicated that the purpose of the attacks was to gain access to source codes of the attacked companies, especially the version management software Periscope used by hundreds of large software companies. McAfee discerned several stages in the attack:[27]

a. The operators of the attacked computer would receive a harmless-looking email or notification from what appeared to be a safe source.
b. The operator would take the bait and click on the link attached to the notification leading to a server containing malware.
c. The web browser in the attacked computer would download a binary code camouflaged inside a picture file and operate a back door that would connect to a control server located in Taiwan.
d. As a result, the attackers would gain full control of the computer and thus also to sensitive information communicated through the network.

This method was widely used in many of the attacks known as APTs (advanced persistent threats). At first, the term indicated sophisticated attacks on military and government networks, but currently the term is used to mean attacks of high intensity (i.e., state-level intensity) on a civilian target.

The Night Dragon and Shady RAT Attacks

These waves of attacks started in mid 2006 and continued until February 2011. McAfee, which gained access to one control server used by the attackers, identified the server after a log file analysis[28] and determined that some 70 targets had been attacked.[29] Given that McAfee gained access to only one control server, the attack presumably targeted many others as well. The analysis mapped the companies attacked and the time frames that the computers were controlled by a server through which the attackers extracted sensitive information. The targets included: 21 government organizations, 6 industrial and energy companies, 13 communication, computer, and electronics companies, 13 security companies, and 6 financial companies. In this context, the attacks on the Norwegian oil and gas companies are particularly noteworthy.[30] Attacks on companies considered national infrastructures, such as energy companies, could be evidence of the desire to create access for the purpose of damaging them at some point in the future.

RSA Attack

The RSA attack provides the basis for an in-depth analysis because one of the servers involved was a botnet[31] of some 2,000 computers. Penetrating the botnet's central server made it possible to analyze the list of infected computers; the analysis generated a list of 763 companies.[32] The attack was first reported by RSA in March 2011.[33] The stages of the attack, typical of other attacks as well, can be charted as follows:

Extensive infrastructure intelligence gathering ➔	Constructing the profile of the attacked computer's owner ➔	Sending email to attacked computer's owner ➔
Installing a back door in the computer ➔	Gathering initial information and expanding the attack ➔	Extensive information gathering

The first stage involves extensive gathering of infrastructure intelligence about the organization targeted. This intelligence is usually gathered from social networks and other open sources. The purpose of the information is to identify potential individual targets, as they will serve as the optimal channels to work within the attacked organization. For example, in the RSA attack, two small groups of employees were selected. They were not necessarily the final targets of the attack but were apparently selected because the attackers felt it would be convenient to start the attack with them.

The next stage involves constructing the profile of the attacked computers' owners: after identifying the penetration points, a profile of those to be attacked is constructed. This requires constructing a full enough picture that allows for the creation of an ostensibly harmless email that would not arouse any suspicion on the target's part. Such information gathering and the construction of a suitable profile require widespread, focused information gathering based on good organizational skills and resources (and especially English language skills).

This is followed by sending malicious email especially adapted to the attacked computer's owner (ZeroDate spear phishing email), which requires two steps. The first entails constructing a formula, structure, and look of a harmless message that would not immediately be erased by the user and would in fact prompt the user to open its links. Email is sent to specific groups of selected employees. At times the message is adapted to every individual user according to the profile constructed. The second action is including an attachment to the email with a security weakness and back door. Weaknesses are software security breaches through which attackers can insert their malicious code. At times the weakness is original, identified in the attacker's weakness identification process (apparently the case with Aurora); at other times, the weakness is well known (ZeroDate) and the attacker relies on the possibility that the targeted computer has not yet installed the patches to fix the weakness.[34] For example, in the RSA attack, the subject line of the email was "Recruitment Plan 2011" and had an Excel document attached, "Recruitment Plan 2011.xls." The ZeroDate weakness was CVE-0609-2011 in Adobe Flash. The moment one of the employees opened the file, the computer was infected via a back door. During the attack the weakness was considered unknown and there was no security update. The update was distributed about a week after the attack.

Installing a back door in the computer: Malicious code is inserted into the infected computer, which allows attackers to control it via a control server.[35] Usually back doors link the attacked computer to the attacker's server, and from there the computer is operated according to instructions from that server based on the commands of the human operators, usually working in shifts. This direction of communication – from within to outside the organization – makes it very difficult to identify the communication.

At this point the attackers gather initial information. Every attacked computer is matched with an attacker group analyzing the computer's contents and trying to assess how to gather information from the attacked computer and what information to gather. At this stage there is usually an assessment of the attacked computer's access to servers and other sources of information within the organization in order to identify the network map and learn how to expand the attack.

The central information gathering stage takes place after access to the company's servers has been gained and the desired information identified. The transfer of large amounts of information in a way that does not arouse suspicion and does not allow identification by monitoring software usually installed by large organizations is highly complex. It is generally done by means of another computer in the network whose access and permissions levels are high enough so that it upgrades the permissions of the servers to export information while using information-compressing encryption and algorithms. For example, in the case of RSA, the attackers finally arrived at a computer that stored sensitive information about the secure ID system, which later allowed the attackers access to information at other companies,[36] all of this bypassing the monitoring systems' warnings about illegal actions.[37]

The approach described herein requires the allocation of many professional resources. It seems that two groups working in tandem with different tools participated in this attack. The first identified the targeted information in the company's network, while the second worked separately to manufacture the channel for extracting the information. A third group, designated to preserve access for later use in the future, may also have been involved. Such an approach reflects the thinking of a world power working with a very high degree of professionalism while investing heavily in resources, such as highly skilled manpower and intelligence capabilities. Indeed, in this attack it is possible to discern some elements suggesting that a world power – presumably China – was behind it. These elements include:

a. *Infrastructure access*: Breaking into a company's one-time password mechanism (OTP) in order to gain access to other companies indicates a desire for extensive action requiring major resources.

b. *Scope of attack*: Open publications reported 763 infected computers found on one of the servers involved in the RSA attack. At least some of the targets required preliminary manual action, i.e., it was necessary to gather preliminary data about the target, construct emails in English that served as bait, and conduct a preliminary analysis of accessibility. An attack of such intensity would have required the organization of infrastructures at the level of a world power, indicating that this was not the work of individual hackers.

c. *The Sykipot back door program*:[38] This program, a variant of PoisonIvy, served Chinese attacks since 2006 (in similar versions) and through early 2012.[39] The use of similar software (with relatively few changes) indicates organizational coordination among the various attackers over the last several years.

d. *Identifying marks*: The back door programs had strong links to China. According to an analysis of the software text, there were clear markers for the Chinese language, including remnants of information in Chinese in binary code (debug information). In addition, error messages in Chinese were identified. Finally, the only user's guide for the back door is in Chinese.

e. *The control servers*: An analysis of the sites where the control servers were placed and from where the attacked computers were controlled showed that most of them were located in China (299 of the 329 control servers).[40]

These findings strengthen the hypothesis that China is behind attacks requiring an extensive, systematic organizational and infrastructure system. Given this, one should not be surprised by the announcement made by General Keith Alexander, the Director of the NSA, which confirmed that China was behind the RSA attack.[41]

The list of 763 companied appearing on one of the servers involved in the RSA attack was analyzed. The analysis included identifying the companies through the internet and characterizing their activities according to three categories: technology companies apparently attacked for the purpose of technological espionage; financial and economic companies that would yield commercial information; and communications providers. These findings usually mean that the infected computer was linked to a public internet service provider (ISP). The analysis showed that close to 80 percent of the companies and organizations attacked were communications providers, while the other 20 percent were split between technological, financial, and other companies. The data indicates a typical botnet breakdown, which includes a very large number of infected computers belonging to private individuals who connected to the internet using an

ISP. The rest of the attacked computers were distributed among some 90 countries, including five in Israel.

Concluding Insights

The series of attacks since 2006 indicate a transition to attacking critical infrastructures, both in the communications and energy fields. Regarding the RSA attack, it is possible that the list of companies on the server included a random botnet list compiled by the Chinese in a lengthy process before the attack was discovered in order to serve as an infrastructure for future attacks. It is possible to send attack email from every infected computer, transfer files, and hide the attacker's identity. However, it is also possible that some of the list is not random and includes companies that are explicitly targeted for attack.

The findings about the attacks in recent years strengthen the research hypothesis that the attacks described are part of a systematic, orderly campaign underway by China. China's cyberspace warfare strategy suits the choice of some of the attack targets, most of all those connected to critical infrastructures. The attack against Google in Aurora, the Shady RAT attacks, and especially the RSA attacks all signal a transition to a systemic approach that targets communications and critical infrastructures. China's strategy, designed to damage the enemy's weaker and lesser-protected realms in a move prior to using kinetic force, requires extensive activity to create long term access to critical infrastructures, including communications. Unlike normally noisy information gathering operations discovered from time to time, it is more difficult to discover operations aimed at infrastructures and gaining access to them for use at some time in the future. It is quite possible that they will never be discovered.

In addition to the attacks discussed above, in April 2011 China was accused of intercepting no less than 15 percent of all internet traffic.[42] Therefore, this activity is likely part of attacks designed to create intelligence access to internet traffic and intercept transmissions before they are encrypted. Moreover, the conclusions of this essay are based on knowledge accrued as the result of analysis of information about attacks that were discovered and publicized. Because some attacks are not discovered and others are discovered but not publicized, one may assume that China is running other cyberspace operations. It is hard to know what exactly is taking place at the companies under attack. One possibility is that they have been fitted with back doors different from the ones used to preserve access and that this back door will be put into action at the attackers' discretion in order to damage the relevant communications infrastructure. Moreover, a sleeper back door is virtually undetectable by existing defensive technologies such as various anti-virus programs.[43]

This is particularly serious with regard to the United States, where there tends not to be a physical separation of communications networks. In other words, the so-called civilian internet[44] is also frequently used in the computer systems of sensitive installations and organizations, and even critical national infrastructures such as electricity producing nuclear reactors and transportation infrastructure control systems. Furthermore, in some cases the United States security systems make extensive use of civilian internet infrastructures, and the separation of networks of sensitive operational systems is not sufficiently developed. This is an essential security weakness allowing attackers a great deal of access to these infrastructures by means of attacking less protected civilian systems. This means the creation of the ability to severely disrupt information transmission at some unspecified future date. Because of this weakness, preliminary damage to communications and telephony infrastructures during a confrontation is liable to disrupt operational and security systems based on these infrastructures.

The response to this weakness requires adopting a comprehensive systemic approach. Attempts to improve the defenses of communications infrastructure providers are insufficient to prevent future attacks. The use of the internet for communications of sensitive systems cannot be based solely on access permissions. No matter how protected, these permissions represent a severe security breach. One of the important components of a response to the weakness described herein lies in differentiated communications networks. It seems advisable to isolate operational networks of the whole gamut of critical systems, such as security systems, operational communications systems, and command and control systems of installations identified as critical national infrastructures. The ability to operate control systems of critical installations through the internet is liable to prove to be a serious problem the moment a sophisticated attacker decides to use back doors at some future point.

Notes

1 Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, October 9, 2009, p. 67.

2 Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, The Brookings Institution, February 2012.

3 On the attack on Mitsubishi Ltd. in Japan in August 2011, see Hiroko Tabuchi, "U.S. Expresses Concern about New Cyberattacks in Japan," *New York Times*, September 21, 2011, http://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html?_r.

4 "Chinese Hacked French Ministry for G20 Data," *The Week*, March 8, 2011, http://www.theweek.co.uk/technology/7229/chinese-%E2%80%98hacked-french-ministry-g20-data%E2%80%99.

5 Erik Helin, "Fingers Point to China in Australian Prime Minister Hack," *Brick House Security,* March 30, 2011, http://blog.brickhousesecurity.com/2011/03/30/australia-pm-hack.

6 On the attack on Canadian government sites, see Greg Weston, "Hackers Attack Canadian Government," *CBS News,* February 16, 2011, http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html.

7 John Markoff and David Sanger, "IMF Reports Cyberattack Led to 'Very Major Breach,'" *New York Times,* June 11, 2011, http://www.nytimes.com/2011/06/12/world/12imf.html.

8 Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time US*, August 25, 2005, http://www.time.com/time/nation/article/0,8599,1098371,00.html.

9 Dimitri Alperovitch, "Revealed: Operation Shady RAT," Version 1.1, McAfee, 2011, http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat.

10 DeWeese, *Copability of the People's Republic of China to Conduct Cyber Warfare*, p. 69.

11 Integrated network electronic warfare.

12 Tim Stevens, "Breaching Protocol: The Threat of Cyberespionage," *Jane's Intelligence Review*, March 2010, pp. 8-13.

13 Timothy L. Thomas, "Chinese and American Network Centric Warfare," *Joint Forces Quarterly* 38, p. 77, http://www.dtic.mil/doctrine/jel/jfq_pubs/1538.pdf.

14 DeWeese, *Copability of the People's Republic of China to Conduct Cyber Warfare*, p.31; Mark A. Stoke, Janny Lin, and L. C. Russell Hsiao, *The Chinese PLA Signal Intelligence and Cyber Reconnaissance Infrastructure,* Project 2049 Institute, 11, 2011, pp. 6-14.

15 It is difficult to verify this assessment.

16 James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai, and Andrew Scobell, eds., *Beyond the Strait: PLA Missions Other than Taiwan* (Washington, DC: National Bureau of Research, 2009), p. 273.

17 In Mandarin: Hikè 黑客, literally "black guest."

18 Stevens, "Breaching Protocol," pp. 8-13.

19 Timothy L. Thomas, "Comparing US, Russian and Chinese Information Operations Concepts," *Foreign Military Studies Office*, Fort Leavenworth, KS 66048, February 2004, pp. 12-13.

20 Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, March/April 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page0,6.

21 See publications on China's cyberspace espionage against the Tibetan government in exile and the break-in of the Dalai Lama's computer infrastructure; Stevens, "Breaching Protocol," pp. 8-13.

22 In the context of this essay, this term denotes the ability to deceive the owner of the computer under attack by creating a posture that fits the user's profile so that the computer will take action that interests the attacker, e.g., respond to email addressed to the owner in a way that is contrary to the security policy of the organization in which s/he works.

23 DeWeese, *Copability of the People's Republic of China to Conduct Cyber Warfare,* p. 60.

24 Eric Chien and Gavin O'Gorman, *The Nitro Attacks, Stealing Secrets from the Chemical Industry,* Symantec Security Respond, 2011, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.

25 It is possible that there was no connection between the hacking of the Gmail accounts of individuals and the attack designed to access the Google and Adobe source codes.

26 Ariana Eunjung Cha and Ellen Nakashima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," *Washington Post*, January 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

27 McAfee Labs and McAfee Foundstone Professional Services, *Protecting Your Critical Assets, Lessons Learned from "Operation Aurora,"* http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf.

28 Log files are files that continuously and automatically document defined computer activity.

29 Alperovitch, "Revealed," p. 3.

30 "Hackers Attack Norway's Oil, Gas and Defence Businesses," *BBC News*, November 18, 2011, http://www.bbc.co.uk/news/technology15790082-.

31 A botnet is a collection of software agents installed on host computers. In many cases these are infected computers that contracted the software agent without the computer owner's knowledge. The software agents can be operated under previously defined conditions or by commands coming from a control server.

32 Brian Kerbs, "Who Else Was Hit by the RSA Attackers," October 2011, http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers.

33 Uri Rivner, "Anatomy of an Attack," April 1, 2011, http://blogs.rsa.com/rivner/anatomy-of-an-attack.

34 ZeroDate weaknesses are software security breaches publicly identified and noted. Usually, as soon as the breach becomes known, the software developer provides a response in the form of a security patch distributed to the public. There is generally a gap between the time the patch is distributed and the time it is actually installed on users' computers. The window of opportunity for attackers starts when the weakness is announced and lasts until the patch is installed on the targeted computer. During this timeframe, attackers can insert malicious code through the breach.

35 Around November 2010, some of the computers of the companies under attack were already in communication with the attackers' control networks.

36 One of the companies attacked using information gathered in the RSA attack was Lockheed Martin. See Mathew J. Schwartz, "Lockheed Martin Suffers Massive Cyberattack," *Information Week*, May 31, 2011, http://www.informationweek.com/news/government/security229700151.

37 Large organizations usually have systems that monitor computer network traffic in order to identify behavior that is illegal according to predetermined rules. Such systems have different commonly used names, including SEIM (security event and information management) and NBA (network behavior analysis). These programs have a set of rules designed to alert administrators to non-permitted or unusual network behavior and also to prevent it from occurring.

38 Stephen Doherty et al., "The Sykipot Attacks," December 14, 2011, http://www.symantec.com/connect/blogs/sykipot-attacks.

39 Mathew J. Schwartz, "More Sykipot Malware Clues Point to China," *Information Week*, December 21, 2011, http://www.informationweek.com/news/security/attacks232300940/.

40 Kerbs, "Who Else Was Hit by the RSA Attackers."

41 Nicholas Hoover, "NSA Chief: China behind RSA Attacks," *Information Week*, March 27, 2012, http://www.informationweek.com/news/government/security232700341/.

42 Stew Magnuson, "Cyber Experts Have Proof that China hs Hijacked U.S.-Based Internet Traffic," *National Defense,* December 11, 2010, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID249=.

43 Gunter Ollmann, *Serial Variant Evasion Tactics Techniques Used to Automatically Bypass Antivirus Technologies*, Damballa, 2009,http://www.damballa.com/downloads/r_pubs/WP_SerialVariantEvasionTactics.pdf.

44 The concept of "civilian internet" denotes internet communications networks used by the public at large and having no particular protection.