Integrated Network Electronic Warfare: China's New Concept of Information Warfare

*Deepak Sharma**

The People's Liberation Army (PLA) considers active offence to be the most important requirement for information warfare to destroy or disrupt an adversary's capability to receive and process data. Launched mainly by remote combat and covert methods, the PLA could employ information warfare pre-emptively to gain the initiative in a crisis. Specified information warfare objectives include the targeting and destruction of an enemy's command system, shortening the duration of war, minimizing casualties on both sides, enhancing operational efficiency, reducing effects on domestic populations and gaining support from the international community. The PLA's Information Warfare (IW) practices also reflect investment in electronic countermeasures and defences against electronic attack. 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 Electronic Warfare (EW). China's Computer Network Operations (CNO) include computer network attack, computer network defence, and computer network exploitation. The PLA sees CNO as critical to seize the initiative and achieve "electromagnetic dominance" early in a conflict, and as a force multiplier. Although there is no evidence of a formal Chinese CNO doctrine, PLA theorists have coined the term "Integrated Network Electronic Warfare" to outline the integrated use of electronic warfare, CNO, and limited kinetic strikes against key command and control, communication and computers nodes to disrupt the enemy's battlefield network information systems. The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks.

Introduction

Network-Centric Warfare (NCW) now commonly called Network-Centric Operations is a universal military doctrine or theory of war. It seeks to translate an information advantage, enabled in part by information technology, into a

* Colonel Deepak Sharma is a Research Fellow at the Institute for Defence Studies and Analyses, New Delhi.

competitive war fighting advantage through the robust networking of well informed geographically dispersed forces. To achieve tenants of NCW a robust and reliable multi-layered communication network for flow of information and integration of sensors, shooters and command and control elements, is an essential requirement of any force of the future.

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 Electronic Warfare (EW).

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 defence 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.

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 Electronic Warfare (EW) under 4th Department (Electronic Countermeasures) of PLA General Staff Department (GSD). The Computer Network Defence (CND) and intelligence gathering responsibilities are likely to be with the GSD 3rd Department (Signals Intelligence), and possibly a variety of the PLA's specialized IW militia units[1].

The PLA Science and Engineering University provides advanced information warfare and networking training and also serves as a centre for defence related scientific, technological, and military equipment research[2]. Recent IW related faculty research has focused largely on rootkit design and detection, 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[3].

Chinese Computer Network Operations Strategy

The Chinese 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 decision-making 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 Informationzed 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. The concept allows the PLA to network its existing force structure without radically revising current acquisition strategies or order of battle[4].

The PLA's doctrine for fighting Local Wars Under Informationzed 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.

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 Informationzed Conditions doctrine[5].

Key Departments Dealing with INEW

General Staff Department Fourth Department. The GSD 4th Department, also referred to as the Electronic Countermeasures Department (ECM), 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

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

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[6]. The GSD's decision in 2000 to promote Dai Qingmin to head the 4th Department vetting his advocacy of the INEW strategy 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 deals in signals intelligence (SIGINT) role and its large staff of trained linguists and technicians make 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[7]. 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 defence as well, though little information is available to confirm this role[8].

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.

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[9].

PLA Information Warfare Militia Units

Since 2002, the PLA has been creating IW militia units[10] comprising of personnel from the commercial IT sector and academia. These units represent an operational nexus between PLA CNO operations and Chinese civilian information security (infosec) professionals. 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 as one of the Guangzhou militia's primary mission[11]. 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. 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.

Cyber-Espionage Techniques

The Chinese academic community and hacker[12] groups like many such groups around the world are heavily focused on researching new zero-day vulnerabilities[13]. 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. 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[14].

The Chinese academic community and hacker groups like many such groups around the world are heavily focused on researching new zero-day vulnerabilities.

Henan Provincial Public Security Bureau authorities had 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[15]. The Black Eagle leadership also expressed appreciation to the State Security Bureau (guojia anquan ju) and the Commission of Science and Technology in National Defence (COSTIND, and now renamed SASTIND) for the educational guidance they provided to members while in custody. The latter, entity, charged with overseeing national defence industry policy, is not typically referenced in connection with hacker groups or their activities.

Individuals, or possibly groups, engaged in computer network exploitation networks have obtained malicious software developed by Chinese underground or black hat[16] 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.

Individuals, or possibly groups, engaged in computer network exploitation networks have obtained malicious software developed by Chinese underground or black hat programmers.

Open source research on the screen name of the coder who created the malware used in the early 2009 attack on US firm revealed that the individual was 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[17].

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[18], 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, programmes, 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. 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.

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[19].

The overall effort likely consists of multiple groups and skilled individuals operating against different targets. 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[20].

The overall effort likely consists of multiple groups and skilled individuals operating against different targets.

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 to be 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, 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.

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.

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.

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[21].

Conclusion

War will continue to be a dangerous and violent clash, while improved information will tend to facilitate a more economical use of force. Information is not an end in itself. Rather, it is a means to an end, and increasingly nations will view that end as the achievement of an effect, whether it be diplomatic, military, economic, informational, societal, technological, or a combination of these instruments of national power. In a war fighting sense, sensor technologies have extended the engagement envelope; computers and communications technologies have led to an increase in the tempo of operations; and the integration of sensors into weapons has made them more precise and lethal. The real transformation, therefore, has not been in sensor, weapons or IT per se, but in shifting the focus from the physical dimension to the information dimension. As China's cyber-attack capability becomes clearer, there is a need to acknowledge the vulnerability of national security information infrastructure, commercial, financial and energy information networks. We, therefore, need to initiate requisite actions to mitigate the threat. The threat is global and the entire computing industry needs to work

together to improve security of information network, as businesses continue facing cyber-attacks.

Experts believe that hardware, software, and networks can be made much safer by creating a multi-layered solution. Bill Gates has suggested replacing password protections, often too easily defeated by phishing and other forms of low-tech hacking, with an Info-Card a digital identity that can be stored in the microchip of a smart card and used to access password-protected websites[22].While the Info-Card technology should be useful for personal data security, large institutions, such as banks, are looking at large-scale defences to tackle Internet scams. While creating more secure technology requires the coordination of software, networks, and hardware, cryptography is at the heart of it. Comprehensive protection against the entire range of threats and risks at all times is virtually impossible, not only for technical and practical reasons, but also because of the associated costs. What is possible is to focus protective measures on preventive strategies and on trying to minimise the impact of an attack when it occurs. A key problem currently is that standard procedures do not exist for assessing the risks to critical infrastructure or for recommending security improvements. Furthermore, a framework for agreeing priorities for security remediation of those critical infrastructures deemed the most vulnerable does not exist.

For defence forces, it is prudent to have an exclusive secure network, fully separated from internet/other networks. In addition, other state-of-the-art network safeguards should also be adopted to protect the network from unwanted intruders.

Explanation of Some Important Terminologies

Type	Description
Spamming	Sending unsolicited commercial email advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malware and other cyber-threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. Internet scammers use email bait to 'phish' for passwords and financial data from Internet users.

Type	Description
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.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. Email spoofing occurs when the sender address and other parts of an email header are altered to appear as though the email originated from a different source. Spoofing hides the origin of an email message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate website. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed website when the user types in a legitimate web address. For example, one pharming technique is to redirect users—without their knowledge—to a different website from the one they intended to access. Also, software vulnerabilities may be exploited or malware employed to redirect the user to a fraudulent website when the user types in a legitimate address.
Denial of Service	An attack in which one user takes up so much of a shared resource that none of the resource is left for other users. DS attacks compromise the availability of the resource.
Distributed Denial	A variant of the DS attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Viruses	A program that 'infects' computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwitting) to propagate.

Type	Description
Trojan horse	A computer program that conceals harmful code. It usually masquerades as a useful program that a user would wish to execute.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Malware	Malicious software designed to carry out harmful actions. Malware often masquerades as useful programs or is embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.
Spyware	Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorised third party.
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for 'robots') are programs that are covertly installed on a targeted system allowing an unauthorised user to remotely control the compromised computer for a variety of malicious purposes.

(Source: GAO, CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats, pp. 7–8)

Notes:

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*

2 *"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

3 "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

4 China's National Defence 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

5 China's National Defence 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 Defence 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/newschannels/2006-12/29/content_691844.htm

6 Mulvenon, PLA Computer Network Operations, p. 272.

7 Desmond Ball, "Signals Intelligence In China" Jane's Intelligence Review, 1 August, 1995

8 HK Journal Details History, Structure, Functions of PRC Intelligence Agencies," Hong Kong Chien Shao, No 179, 1 January, 2006.

9 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.apaninfo.net/Portals/45/VIC_Products/2006/08/060804-P-China.doc.

10 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 Defence in 2004, Information Office of China's State Council, December 2004,

http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html | China's

National Defence 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/newschannels/2006 12/29/content_691844.htm "Telecom Experts in Guangzhou Doubling As Militia Information Warfare Elements," Guofang, Academy of Military Science, 15 September, 2003.

11 Lu Qiang, "Focus On The Characteristics Of Information Warfare To Strengthen The City Militia Construction" China Militia Magazine, August 2003, available at: http://www.chinamil.com.cn/item/zgmb/200308/txt/16.htmZ

12 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. 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 disrupt the 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 oractually penetrate networks; this group also falls into the same two subcategories as above. Their goal is also profit (See:

http://www.uscert.gov/control_systems/csthreats.html).

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

Hacktivist. An attacker who practices hacktivism.

13 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.

14 Scott Henderson, The Dark Visitor, p.29

15 US-China Economic and Security Review Commission

Report on the Capability of the People's Republic of China to

Conduct Cyber Warfare and Computer Network Exploitation October 9, 2009

http://news.cnet.com/8301-13639_3-10381621-42.html?part=rss&subj=news&tag=2547-1_3-0-20

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

17 *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.*

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

19 *http://www.securityfocus.com/columnists/470 and http://www.eweek.com/c/a/Security/Hackers-Selling-Vista-ZeroDay-Exploit/ for additional background.*

20 *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*

21 *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

22 *Kate Greene, 'Calling Cryptographers', MIT Technology Review, 16 February 2006, available at <http://www.technologyreview.com/Infotech/ 16347/?a=f>, accessed 4 March 2008.*