China's Cyber Warfare Capability and India's Concerns

*Deepak Sharma**

The Chinese cyber warfare department's multiple agencies and individuals are seriously working towards the overall objective of instantly disrupting or at least weakening the adversary's computer networks so as to paralyse his decision making capability at the very commencement of hostilities. It is very difficult to protect networks from such attacks. The weakest link in cyber security measures are the persons operating the system who often, knowingly or unknowingly, default on cyber security measures. It is possible for defence to have an exclusive secure network with air gap from civil and public networks which ensures that the adversary is not allowed to even access its periphery.

Introduction

Strategic communications systems, on which depends the very survival of the country, must not only be fail safe and secure under normal circumstances, but also be so even when under attack from those who have set up these systems and have inside knowledge. The modern information technology has created a global village. Every thing on the information network is data, whether voice or video, and varies in the protocols they follow. Hence the data that flows either from computers or telephones from one location to other over the network is a part of the communication and overall network system. As the defence forces enter the network centric warfare (NCW) era, their dependence on fail safe and secure broadband communications capable of handling voice, data, and video increases.

In March 2011, the government of India asked mobile operators to change the SIM cards of all mobile phones to indigenously made SIMs, as foreign SIMs could contain embedded worms which could adversely affect the functioning of cellular networks.[1] It is important to understand that cyber space is no different from the information or communication space. It is actually a subset of communication systems and networks. Most modern networks have a centralised management

Most modern networks have a centralised management system, to manage, and control all the resources of network.

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

system, to manage, and control all the resources of network. Anyone with access to the network management system irrespective of physical location within the network can pose a great potential threat to the network when it is needed the most. The management information is generally in clear text mode when bandwidth or lamda is hired from a service provider. Such network management systems can be easily hacked and corrupted to disable the network whenever required.

Anyone with access to the network management system irrespective of physical location within the network can pose a great potential threat to the network

The government of the People's Republic of China (PRC) is a decade into a sweeping military modernisation programme that has fundamentally transformed its ability to fight high tech wars. China's modernisation plans for its armed forces include the development of a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum.[2]

The PLA Science and Engineering University serves as a centre for defence related scientific, technological, and military equipment research. The university also provides advanced information warfare and networking training.[3]

The Information Warfare (IW) faculty has recently focused its research on rootkit design and detection, including rootkit detection on China's indigenously developed Kylin operating system. The PLA Information Engineering University provides PLA personnel advanced technical degrees and training in all aspects of information systems, including information security and information warfare.[4]

The IW strategy of PLA is geared towards the combined employment of network warfare tools and electronic warfare weapons against an adversary's information systems in the early phases of a conflict.

Information Warfare Strategy

The IW strategy of PLA is geared towards the combined employment of network warfare tools and electronic warfare weapons against an adversary's information systems in the early phases of a conflict. China's military has shifted its focus from its reliance on massed armies of the Maoist era People's War Doctrine and is becoming a fully mechanised force linked by advanced fully integrated and networked technologies. Informationisation is essentially a hybrid development process, continuing the trend of mechanisation and retaining much of the current

force structure, while overlaying it with advanced information systems 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.[5]

To fight an 'information' war the Chinese have adopted the "Integrated Network Electronic Warfare" (INEW), a formal IW strategy which guides the employment of computer network operations (CNO) and related information warfare tools. The INEW encompasses 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 with other PLA specialised IW militia units[6].

Key Entities in Chinese Computer Network Operations

GSD 4th department: Offensive EW is the GSD 4th department's traditional role. According to open source reporting the department is now responsible for implementing INEW, for offensive IW in the PLA.

GSD 4th department: Offensive EW is the GSD 4th department's traditional role. According to open source reporting the department is now responsible for implementing INEW, for offensive IW in the PLA. The 4th department, also referred to as the Electronic Countermeasures Department (ECMD), oversees both the operational ECM units and R&D institutes conducting research on a variety of offensive IW technologies. The 4th department's oversight of IW dates back to at least 1999 and probably earlier. The GSD's decision in 2000 to promote Dai Qingmin to head the 4th Department suggests that the GSD probably endorsed his vision of adopting INEW as the PLA's IW strategy.[7]

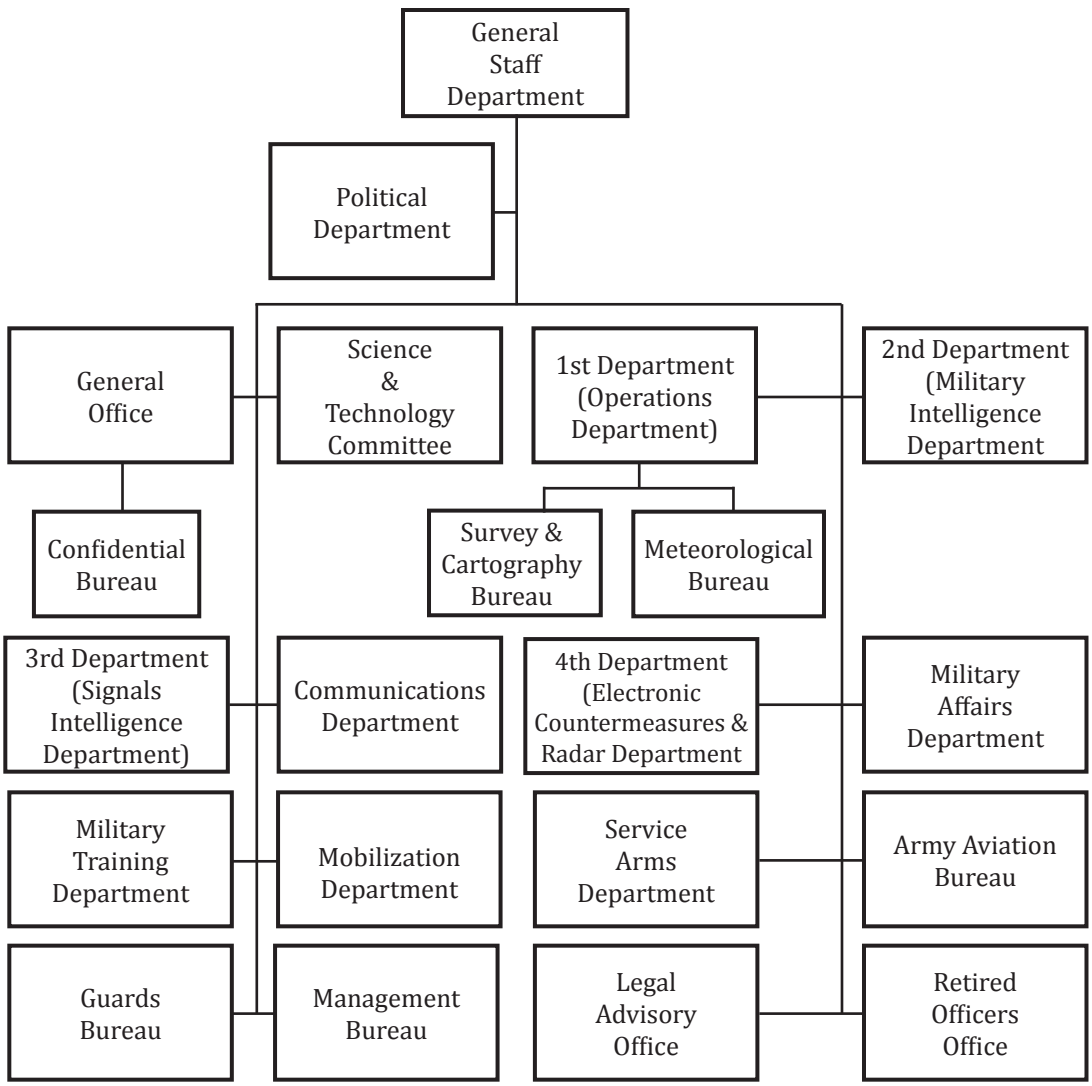
GSD 3rd Department: The GSD 3rd department is responsible for signals intelligence (SIGINT) gathering, and primarily focuses on defensive operations. Its large staff of trained linguists and technicians make it well suited for oversight of CND missions in the PLA. The 3rd Department controls an extensive system of signals collection stations throughout China with collection and processing stations co-located with each of the PLA's military region headquarters.[8]

The 3rd Department controls 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.[8]

It is tasked with foreign signals collection, exploitation, and analysis and also communications security for the PLA voice and data networks. This latter responsibility may encompass network defence as well, though little information is available to confirm this role.[9]

Technical Reconnaissance Bureaus: The PLA maintains at least six technical reconnaissance bureaus (TRB) located in 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 of the exact role or subordination of these units.[10]

General Staff Department of the People's Liberation Army: The details of various departments of GSD are given as per the chart given as under.[11]



PLA Information Warfare Militia Units: The PLA has been creating IW militia units since 2002.[12] The units have personnel from the commercial IT sector and academia. This indicates that an operational nexus exist between PLA CNO operations and Chinese civilian information security (infosec) professionals. In 2003 a political commissar for the Guangzhou People's Armed Police (PAP) garrison advocated the need for direct involvement of urban militia units in information warfare, electronic warfare, and psychological warfare. He also proposed that militia reform efforts should focus on making information warfare one of the primary missions of the Guangzhou militia. PLA media reports indicate that IW militia units are tasked with offensive and defensive CNO, and EW responsibilities, and psychological warfare, and deception operations. In March 2008, a militia battalion in Yongning County (Ningxia Province, Lanzhou Military Region) established an IW militia group and tasked it to conduct network warfare research and training, and to attack the enemy's wartime networks.[13]

PLA media reports indicate that IW militia units are tasked with offensive and defensive CNO, and EW responsibilities, and psychological warfare, and deception operations.

Chinese Computer Network Operations Strategy

The Chinese People's Liberation Army (PLA) is creating tools for strategic guidance and training personnel necessary to support traditional war fighting disciplines, and is developing CNO capability. The PLA has not openly published a CNO strategy with the formal vetting of the Central Military Commission (CMC), which is China's top military decision-making body, or the Academy of Military Sciences (AMS), its leading body for doctrine and strategy development.

Cyber-Espionage

The Chinese academic community and hacker groups like such groups around the world are heavily focused on researching new 'zero-day' vulnerabilities. Reports from information security industry sources suggest that Chinese researchers are also willing to purchase zero day attack tools from third parties, though this has not been independently corroborated. White hat information security researchers (i.e. those pursuing overt legal research in the field) are developing extensive government customer bases for hardware and

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

possibly software support. Many of the most prominent earlier groups and their leaders have either disbanded or transformed themselves into seemingly legitimate security firms. Large groups like Xfocus and Black Eagle Base have reinvented themselves as commercial operations, in line with state security and information security objectives. NSFocus, which is 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 the logo of the Green Army Alliance and the list of its founding members features some of the most prominent hackers in China.[14]

In February 2006, the Henan Provincial Public Security Bureau authorities arrested members of the Patriot Hackers-Black Eagle Base and shut down its web site. The group, however, was operational again six months later as Black Eagle Honker Base. Its members in a statement claimed that the group would focus its efforts on training people for the state and work to improve the state's network security industry. This shows a possible cooperative relationship with state authorities as a condition for their release.[15] The Black Eagle leadership also commended the State Security Bureau (guojia anquan ju) and the Commission of Science and Technology in National Defence (COSTIND, now renamed SASTIND), for the guidance they provided to members while in custody.

Cyber-Espionage Methodology

In one proven instance, black hat programmers affiliated with Chinese hacker forums provided malicious software to intruders targeting a US commercial firm in early 2009. According to forensic analysis, the techniques and tools employed by this group or individuals were similar to those observed in previous penetration attempts against this same company in 2008. Forensic analysis also revealed that this group comprised of multiple members with varying skill levels, operating with fixed schedules and standard operating procedures and were willing to intricate steps to mask their activities on the targeted computer. Chinese underground or black hat programmers have probably helped individuals, or possibly groups, engaged in computer network exploitation to develop malicious software. The ability to obtain this custom code indicates that these operators have ties with select members of the hacker underground.

The ability to obtain this custom code indicates that these operators have ties with select members of the hacker underground.

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 to be a native Chinese speaker. A key stroke logging programme with rootkit

elements was posted to a discussion board on a prominent Chinese hacker group website - EvilOctal. The coder used FreePic2Pdf, version 1.26 F - a tool that is only available in Chinese – to carry the malicious software. This document was modified to covertly install a (the Trojan horse) zero day exploit that targeted a previously unknown vulnerability in Adobe Acrobat.[16] 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 recognised between this computer and previously compromised systems on the same network, the attack team extracted small amounts of data to determine the configuration of security software installed and their ability to access targeted data on the company's network. The operators installed a rootkit, which gives the attacker privileged access to a victim computer while remaining indetectable, suggesting that 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 operator's files, programmes, network connections and registry settings. However, an 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.[17]

This implies that multiple groups and skilled individuals generally operate against different targets. The adversaries associated with this issue are successful because they are able to maintain a presence on a targeted network for extended periods.

The scale and complexity of targeting associated with the above effort suggests that it is probably backed by a mature management bureaucracy. They are able to collate and disseminate collection priorities to diverse teams of operators, intelligence analysts, and malware developers.

This implies that multiple groups and skilled individuals generally operate against different targets. The adversaries associated with this issue are successful because they are able to maintain a presence on a targeted network for extended periods. They 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 to craft specific, seemingly legitimate looking, emails to targeted users. 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 analysing their emailing patterns. The operators often reuse the employee profiles so 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 target who usually opens these emails and thus represent a reliable entry vector for the intruders. The intruders craft credible emails from members or groups within an individual's network that the target will likely open. The emails usually contain either malicious software embedded in an attachment or links to malicious websites 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 programme on the victim's computer (e.g. PowerPoint, WordPad, Adobe Acrobat, etc), the backdoor programme executes.[18] This initial penetration with email and malicious attachment is 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.

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 analysing their emailing patterns.

Task Oriented Structure: Some operations involve multiple individuals who are responsible for specific tasks such as gaining and establishing network access, surveying portions of the targeted network to identify information of value, and organising data exfiltration. There is an entry or breach team tasked only with gaining entry and maintaining a flexible, redundant presence in the target network. Their job is 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. Additional individuals or teams probably tasked with the collection of the actual targeted information

have greater skill and highly detailed knowledge of the targeted networks. Their efforts to locate and move data off the network often involves techniques that place a premium on redundancy, stealth and comprehensiveness of preparation and attention to detail. Using network intelligence, which has been gathered during earlier reconnaissance efforts, the 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 organisation, to multiple external servers that act as drop points. These drop points may also play an obfuscating role, ensuring that investigators are unable to identify the data's final destination[19].

Reasons for using different individuals or groups therefore could be due to the specialised skills required for each phase of an intrusion or perhaps for compartmentalisation 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 ensuring 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 model, if accurate, also implies some means of recruiting, organising, and managing a special team and ensuring proper completion of a given mission. If this model is indeed accurate and being replicated across dozens of intrusions over time, then the oversight structure should also be proportionately as extensive and complex.

Chronology of Alleged Chinese Computer Network Exploitation Events Targeting Foreign Networks 2009

March 2009: A Canadian research team publishes a study of the GhostNet cyber espionage network that targeted over 1,300 hosts around the world including the German, Indian, Pakistani and Portuguese embassies around the world and the Tibetan government in exile in India. The Canada-based Information Warfare Monitor (IWM) notes the compromising of numerous government and private information processing systems across 103 countries. The network operated from Hainan Island in China. The Chinese government denies all accusations of responsibility or state sponsorship.[20]

March 2009: The *Philippine Daily Inquirer* publishes a report citing GhostNet that the computer network of the Philippines' Department of Foreign Affairs (DFA) has been hacked by cyber spies based in China.[21]

April 2009: Media reports claim that the German government records daily attacks against its networks, many from China based operators. The German foreign office is particularly targeted; the reports note that these are penetrated via a social email.[22]

April 2009: The Australian media reports that Chinese cyber spies are targeting the Australian prime minister via email and mobile phones. The Chinese government denies all accusations.[23]

April 2009: Media sources report that hackers based in China infiltrated the Intranet of the South Korean finance ministry, creating concerns regarding the potential theft of sensitive government data. The cyber attackers used socially engineered emails to target ministry staff. The emails, disguised to look as though sent from one or more trusted officials, executed malicious software when opened allowing the attackers to access the systems.[24]

On January 19, 2010, M.K. Narayanan, the then National Security Advisor of India, in an interview to *Times magazine*, revealed that his office and other government departments were targeted on December 15, 2009 - the same date on which Google reported sophisticated cyber attacks from China. A Trojan virus which allows a hacker to access a computer remotely and download or delete files was embedded in an e-mail PDF attachment. The virus was detected and officials were told not to log on until it was eliminated. It was suspected to be of Chinese origin though China denied any role in such an attack on Indian systems.[25] There have also been other instances of cyber attacks in the past, on the sites/computers of ministry of external affairs (MEA), ministry of home affairs (MHA), and ministry of defence (MoD) by unknown hackers. This was possible because these agencies groups or individuals were able to access the network through the communication system supporting these computer systems.

Recommendations

From the foregoing discussion it is clear that whatever the source of the cyber attack -China, Pakistan or any other agency, the first and foremost priority measure is to protect the network by restricting the entry of unknown users at the physical level of connectivity of network. The Chinese have an advanced capability to attack the adversary's network which can seriously jeopardise the national and other network dependent civil operations of that country, and India is not an

Whatever the source of the cyber attack -China, Pakistan or any other agency, the first and foremost priority measure is to protect the network by restricting the entry of unknown users at the physical level of connectivity of network.

exception to this. Nothing very much can be done to fully secure the civil and public network against cyber attack, but the vulnerability can be curtailed to some extent. However, for defence networks the following measures can be adopted:

a) The network should be planned, owned and operationalised by defence agencies themselves.

b) Total network security must be planned in addition to bulk media secrecy.

c) Network equipment should be procured from reliable original equipment suppliers.

d) Multi-layer communication systems, with redundancy catered for the critical systems at all levels should be installed

e) Only applications on client computers connected on network to ensure security of individual files/data should be maintained.

f) Data/ information can be kept encrypted on detachable seperate hard drive, to be connected through USB port on network computer to transmit particular file only. The file to be transmitted should only be copied on to the computer and once transmitted be securely deleted.

g) Encryption and decryption of data/ file be carried out on separate standalone computer.

The last three points can be adopted by civil users of Internet and other private or public networks.

Conclusion

It is evident that future wars will also be fought in the information domain and cyber space which is a subset of the information domain will automatically be the part of it. As stated earlier the multiple agencies of the Chinese cyber warfare department's are seriously working to attain the overall objective of instantly disrupting or at least weakening the adversary's communication systems to paralyse his decision making capability at the very commencement of hostilities. It is well known that cyber operations are eminently deniable and hence serve Chinese national security objectives without a serious risk of retaliation or even

accusation. China has made major progress in synergising, combining, and coordinating its signal intelligence, EW, information security and computer network attack systems. These efforts have made the Chinese system more effective and secure.

China has made major progress in synergising, combining, and coordinating its signal intelligence, EW, information security and computer network attack systems.

It is very difficult to protect networks from attacks. The weakest link in implementing and ensuring cyber security measures is human as the operators employed quite often default on cyber security measures, whether knowingly or unknowingly. For defence forces it is possible to have an exclusive secure network with air gap from civil and public networks. This will ensure that the adversary is not allowed to even reach the periphery of the defence network. To meet the requirements of interoperatibilty between the various services of the defence force, it should be ensured that the networks observe the same levels of secrecy, and the connectivity between the networks can be through a number of gateways with stringent monitoring and access protocols. In addition to these measures, the available state-of-the-art network safeguards should also be adopted to protect the network from unwanted intruders.

For defence forces it is possible to have an exclusive secure network with air gap from civil and public networks. This will ensure that the adversary is not allowed to even reach the periphery of the defence network.

In the long run, the India has to counter cyber space threats on a number of fronts. One such example is threat from criminals and underworld mafias who are also exploiting the cyber space to support their criminal activities in all the fields ranging from cyber piracy to drugs peddling networks. Another threat is industrial espionage by countries and big corporate for economic gains.

Important Terminologies

Rootkit: Rootkit is software that can be installed, on the victim computer without the user's knowledge and remain hidden. It may be included in a larger software package or installed by an attacker who has been able to take advantage of the 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 programmes, or perform other functions on the targeted computer without being detected[26].

Black Hat: A computer hacker intent on causing damage illegally intruding into a system for unauthorised activities.

Hacker: Commonly the term is applied to people who gain illegal access to others computers.

Script Kiddies: Unskilled attackers who do not have the ability to discover new vulnerabilities or write exploit codes, and are dependent on the research and tools from others.

Worm and Virus Writers: Attackers who write the propagation code used in 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 or actually penetrate networks; this group also falls into the same two subcategories as above. Their goal is also profit.[27]

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

Hacktivist: An attacker who practices hacktivism.

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

Spearphishing: A targeted phishing attack against a select group of victims. Spearphishing is commonly used to refer to any targeted email attack, not limited to phishing.

Trojan Horse: The Trojan Horse is a programme with hidden functions that can exploit the privileges of the user (running the programme). A Trojan horse does things that the programme user did not intend. Trojan horses rely on users to install them, or they can be installed by intruders who have gained unauthorised access by other means. An intruder attempting to subvert a system using a Trojan horse relies on other users running the Trojan horse to be successful.[28]

Zero Day Exploit: An attack against a software vulnerability that has not yet been addressed by the software developer/maintainer. 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. idsa

---

Notes:

1 *The Times of India,* Delhi edition, March 08, 2011.

2 "China's National Defence in 2004," Information Office of the State Council of the People's Republic of China, Beijing, December 27, 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, December 29, 2006, available at http://english.chinamil.com.cn/site2/newschannels/2006-12/29/content_691844.htm

3 "PRC Establishes New Military Schools Per Jiang Decree," *Xinhua News*, July 2, 1999. "China Establishes New Military Schools," *People's Daily*, March 7, 1999, available at http://english.peopledaily.com.cn/english/199907/03/enc_19990703001001_TopNews.html

4 "China Establishes New Military Schools," *People's Daily*, March 7, 1999, available at http://english.peopledaily.com.cn/english/199907/03/enc_19990703001001_TopNews.html

5 "China's National Defence in 2008," Information Office of the State Council of the People's Republic of China, Beijing, December 29, 2008 available at http://www.chinadaily.com.cn/china/2009-01/20/content_74133294.htm

6 The General Staff Department is the highest organisational 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, mobilisation, foreign relations, and management

7 Mulvenon, James, "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,* Carlisle, PA: Strategic Studies Institute, April 2009, p. 272.

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

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

10 Blasko, Dennis, "PLA Ground Force Modernization and Mission Diversification: Underway in all Military Regions," in Roy Kamphausen, Andrew Scobell, eds., *Right Sizing, the People's Liberation Army: Exploring the Contours of China's Military*, Strategic Studies Institute, September 2007, p. 366- 372. Also see Melvin, Ellis L., 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, August 04, 2006, available at http://www1.apaninfo.net/Portals/45/VIC_Products/2006/08/060804-P-China.doc.

11 Finkelstein, David, Organizational chart from "The General Staff Department of the Chinese People's Liberation Army: Organization, Roles, & Missions," in James C. Mulvenon and Andrew N. D. Yang, eds., *The People's Liberation Army as Organization,* Reference Vol. v1.0, , Santa Monica, CA: RAND Corp 2002.

12 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. For deals see "China's National Defence in 2004," Information Office of China's State Council, 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, 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, September 15, 2003.

13 Qiang, Lu, "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.htm

14 Henderson, Scott *The Dark Visitor: Inside the World of Chinese Hackers*, Scott Henderson Publisher, 2007, 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, available at http://news.cnet.com/8301-13639_3-10381621-42.html?part=rss&subj=news&tag=2547-1_3-0-20

16 For details see "Security Updates available for Adobe Reader and Acrobat versions 9 and earlier", February 19, 2009 available at http://www.adobe.com/support/security/advisories/apsa09-01.html. And, "Adobe Reader and Acrobat JBIG2 buffer overflow vulnerability", Vulnerability Note VU#905281, available at http://www.kb.cert.org/vuls/id/905281.

17 Reid, Jamie, "Just Who's Being Exploited?", April 21, 2008, available at http://www.securityfocus.com/columnists/470. And, also see at http://www.eweek.com/c/a/Security/Hackers-Selling-Vista-ZeroDay-Exploit/ for additional background.

18 Grow, Brian, *et al.* "The New E-spionage Threat," *Business Week*, April 10, 2008, available at http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

19 Ibid.

20 Markoff, John, "Vast Spy System Loots Computers in 103 Countries," *The New York Times*, March 28, 2009, available at http://www.nytimes.com/2009/03/29/technology/29spy.html

21 Aning, Jerome and Olchondra, Riza T., "RP Gov't Websites Vulnerable to Hacking," *Philippine Daily Inquirer*, March 2009.

22 Goetz, John and Rosenbach, Marcel, "Cyber Spies: 'GhostNet' and the New World of Espionage," *Speigel Online*, April 2009.

23 "Chinese Diplomat Dismisses Australian 'Cyber Espionage' Claims," *The Australian Online*, April 2009.

24 "China-Based Hackers Access S. Korean Finance Ministry's Intranet," *Asia Pulse News*, April 2009.

25 "Chinese Cyber Attack on India Government Offices Too?", January 19th, 2010, available at http://teck.in/chinese-cyber-attack-on-india-government-offices-too.html#ixzz1GMh5K1jM

26 "Understanding Hidden Threats: Rootkits and Botnets", National Cyber Alert System, Cyber Security Tip ST06-001, available at http://www.uscert. gov/cas/tips/ST06-001.html.

27 "Cyber Threat Source Descriptions", available at http://www.uscert. gov/control_systems/csthreats.html.

28 "Systems Affected", CERT® Advisory CA-1999-02 Trojan Horses, available at www.cert.org/advisories/CA-1999-02.html.