China's Cyber Warfare Capabilities

Desmond Ball

China has the most extensive and most practised cyber-warfare capabilities in Asia. This article describes the development of these capabilities since the mid-1990s, the intelligence and military organisations involved, and the particular capabilities that have been demonstrated in defence exercises and in attacks on computer systems and networks in other countries. It notes that it is often very difficult to determine whether these attacks have originated with official agencies or private 'Netizens'. It argues that China's own computer systems and networks are replete with vulnerabilities, of which Chinese officials are well aware. It concludes that this appreciation of China's deficiencies and vulnerabilities has led to the adoption of a pre-emptive strategy, as practiced in People's Liberation Army exercises, in which China's very destructive but relatively unsophisticated cyber-warfare capabilities are unleashed at the very outset of prospective conflicts.

China has the most extensive and most practiced cyber-warfare capabilities in Asia, although the technical expertise is very uneven. China began to implement an Information Warfare (IW) plan in 1995, and since 1997 has conducted numerous exercises in which computer viruses have been used to interrupt military communications and public broadcasting systems. In April 1997, a 100-member elite corps was set up by the Central Military Commission to devise "ways of planting disabling computer viruses into American and other Western command and control defence systems".[1] In 2000, China established a strategic IW unit (which US observers have called 'Net Force') designed to "wage combat through computer networks to manipulate enemy information systems spanning spare parts deliveries to fire control and guidance systems".[2] The People's Liberation Army (PLA) announced on 20 July 2010 that it had established an 'Information Protection Base' under the General Staff Department. This is probably a 'computer network defence' or 'computer security operations' centre.[3]

Chinese cyber-warfare units have been very active, although it is often very difficult to attribute activities originating in China to official agencies or private 'Netizens' ('*WangMin*'). Since 1999, there have been periodic rounds of attacks against official Web-sites in Taiwan, Japan and the United States. These have typically involved fairly basic penetrations, allowing Web-sites to

[1] Ivo Dawnay, 'Beijing Launches Computer Virus War on the West', *The Age* (Melbourne), 16 June 1997, p. 8.
[2] Jason Sherman, 'Report: China Developing Force to Tackle Information Warfare', *Defense News*, 27 November 2000, pp. 1, 19.
[3] 'The People's Liberation Army's First Force on Strategic Information Support and Protection is Established', *China Review News*, 20 July 2010, <http://www.chinareviewnews.com/doc/1013/8/7/2/101387269.html?coluid=7&kindid=0&docid=101387269&mdate=0720090536> [Accessed 18 May 2011].

be defaced or servers to be crashed by 'Denial-of-Service' (DOS) programs. More sophisticated 'Trojan Horse' programs were used in 2002 to penetrate and steal information from the Dalai Lama's computer network.[4] More recently, Trojan Horse programs camouflaged as Microsoft Word and PowerPoint documents have been inserted in computers in government offices in many countries around the world.[5] Portable, large-capacity hard discs, often used by government agencies, have been found to carry Trojan Horses that automatically upload to Beijing Web-sites everything that the computer user saves on the hard disc.[6] From the late 1990s until 2005, the PLA conducted more than 100 military exercises involving some aspect of IW, although the practice generally exposed substantial short-falls.[7] A similar number was probably conducted in the period from 2005 to 2010.

Any critique of China's cyber-warfare capabilities must necessarily include some assessment of its cyber-intelligence operations. As a report prepared for the US-China Economic and Security Review Commission in October 2009 noted:

> Ultimately, the only distinction between computer network exploitation and attack is the intent of the operator at the keyboard. The skill sets needed to penetrate a network for intelligence gathering purposes in peacetime are the same skills necessary to penetrate that network for offensive action during wartime.[8]

And as Admiral Robert Willard, the Commander-in-Chief of the US Pacific Command (CINCPAC) told the Congress on 13 January 2010, "U.S. military and government networks and computer systems continue to be the target of intrusions that appear to have originated from within [the People's Republic of China]", and "although most intrusions focus on exfiltrating data, the skills

[4] Christopher Bodeen, 'Mainland Asks Taiwan to Stop Interference', *The Washington Times*, 26 September 2002; Doug Nairne, 'State Hackers Spying On Us, Say Chinese Dissidents', *South China Morning Post*, 18 September 2002.

[5] See, for example, 'Outrage in Berlin Over Chinese Cyber Attacks', *Weekly Standard,* 31 August 2007, <http://www.weeklystandard.com/weblogs/TWSFP/2007/08/outrage_in_berlin_over_chinese.asp> [Accessed 18 May 2011].

[6] Yang Kuo-wen, Lin Ching-chuan and Rich Chang, 'Bureau Warns on Tainted Discs', *Taipei Times*, 11 November 2007, <http://www.taipeitimes.com/News/taiwan/archives/2007/11/11/2003387202> [Accessed 18 May 2011], p. 2.

[7] I-Ling Tseng, 'Chinese Information Warfare (IW): Theory Versus Practice in Military Exercises (1996-2005)', MA Sub-thesis, Graduate Studies in Strategy and Defence, Strategic and Defence Studies Centre, Australian National University, Canberra, March 2005.

[8] Bryan Krekel, 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation', Northrop Grumman Corporation, McLean, Virginia, 9 October 2009, <http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf> [Accessed 18 May 2011], pp. 8-9.

being demonstrated would also apply to wartime computer network attacks".[9]

Organisationally, the PLA has consolidated the computer and network attack missions together with Electronic Warfare into an 'Integrated Network Electronic Warfare' (INEW) activity under the General Staff Department's 4th (Electronic Countermeasures) Department. Computer network defence has apparently been included with cyber-espionage in the 3rd (Signals Intelligence) Department. Specialised IW militia units also share some aspects of these missions.[10]

In addition, the Chinese military and intelligence agencies are able to readily utilise the corporate sector, including not only state-owned telecommunications carriers such as China Telecom Corporation but also so-called 'private' companies which provide telecommunications and information technologies and services. For example, Huawei Technologies Company, one of the biggest suppliers of telecom equipment in the world, has been effectively blocked from business in the United States because of accusations by US officials that it is "linked to the Chinese military".[11] Chinese manufacturers of electronic gadgets, such as iPods, digital picture frames, and navigation gear, have also been found to have installed viruses in their products that subsequently send information back to Beijing.[12] And the Chinese authorities have access to the large community of patriotic 'Netizens' which is highly skilled in the design and implantation of Trojan Horse programs and other forms of malicious software ('malware'). (Table 1 is a selected list of some of the worst viruses and worms propagated from 1994 to 2011.)

[9] John T. Bennett, 'Chinese Buildup of Cyber, Space Tools Worries U.S.', *Defense News*, 13 January 2010, <http://www.defensenews.com/story.php?i=4452407> [Accessed 18 May 2011].
[10] Krekel, 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation', pp. 6-7; Desmond Ball, 'China and Information Warfare: Signals Intelligence, Electronic Warfare and Cyber Warfare', in K. Santhanam and Srikauth Kondapalli (eds), *Asian Security and China, 2000-2010*, (New Delhi: Shipra Publications, 2004), pp. 115-41.
[11] Michael Kan, 'China's Huawei to Reverse Controversial Deal for 3Leaf', *ITWorld*, 19 February 2011, <http://www.itworld.com/node/137654> [Accessed 18 May 2011]; John Bussey, 'In Huawei's Bid to Crack Market, U.S. Sees a Threat From China Inc.', *Wall Street Journal*, 28 February 2011, <http://dailyme.com/story/2011022700010554> [Accessed 18 May 2011]; John Markoff and David Barboza, 'Huawei, A Chinese Trojan Horse?', *Chinh's News*, 28 October 2010, <http://chinhdangvu.blogspot.com/2010/10/huawei-chinese-trojan-horse.html> [Accessed 18 May 2011]; and Krekel, 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation', p. 49.
[12] 'Computer Viruses: China's Electronic Gadgets are the Latest Sources', Information Technology Consulting, 27 February 2011, <http://informationtechnologyconsulting.yuiin.com/computer-viruses-chinas-electronic-gadgets-are-the-latest-sources/> [Accessed 18 May 2011].

Cyber-warfare Activities

PLA IW units have reportedly developed 'detailed procedures' for Internet warfare, including software for network scanning, obtaining passwords and breaking codes, and stealing data; information-paralysing software, information-blocking software, information-deception software, and other malware; and software for effecting counter-measures. These procedures have been tested in field exercises since about 2000. For example, 500 soldiers took part in a network-warfare exercise in Hubei province in 2000 in which simulated cyber-attacks were conducted against Taiwan, India, Japan and South Korea. In another exercise in Xian, ten cyber-warfare missions were rehearsed, including planting (dis)information mines; conducting information reconnaissance; changing network data; releasing information bombs; dumping information garbage; releasing clone information; organising information defence; and establishing 'network spy stations'.[13] In Datong, forty PLA specialists were reported in 2001 to be "preparing methods of seizing control of communications networks of Taiwan, India, Japan and South Korea".[14] In October 2000, an exercise presided over by the PLA Chief of Staff simulated cyber-warfare and EW "with countries south and west of [the] Gobi desert".[15] As the US Secretary of Defense reported to Congress in May 2007, "the PLA sees CNO [computer network operations] as critical to achieving 'electromagnetic dominance' early in a conflict". It has incorporated "offensive CNO into its exercises, primarily in first strikes against enemy networks".[16]

The PLA has reportedly established at least twelve facilities for INEW training at unit levels in computer network attack and defence operations, jamming and other forms of electronic warfare, and other IW activities. The 'flagship' facility is evidently located at Zhurihe in the Beijing Military Region, and features an "informationalised Blue Force" for 'opposed force' exercises. During an exercise in the Beijing Military Region in June 2004, for example, the 'Blue Force' used network attacks to seize control of the 'Red Force' command network "within minutes of the start of the exercise, consistent with the INEW strategy's emphasis on attacking enemy C2 [command and control] information systems at the start of combat".[17] An 'opposed force' IW exercise in the Lanzhou Military Region in February 2009 also included computer network attack and defence scenarios.[18]

[13] InfoSec News, 'Battle of the Mouse', Security Focus.com, 20 March 2001, <http://www.infosecnews.org/hypermail/0103/3751.html> [Accessed 18 May 2011].
[14] Ibid.
[15] Ibid.
[16] Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2007*, 23 May 2007, <http://www.defense.gov/pubs/pdfs/070523-china-military-power-final.pdf> [Accessed 18 May 2011], p. 22.
[17] Krekel, 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation', pp. 16-7.
[18] Ibid, p. 17.

Cyber-warfare activities go beyond intelligence collection operations in at least two quite different respects. First, they include a large group of activities designed to damage or destroy network elements, such as Web-sites, hard drives, operating systems and servers, as well as infrastructure dependent upon those elements, such as communications systems, financial services, power grids, air traffic control systems, etc. The simplest of these activities involve Denial-of-Service attacks which overwhelm network devices (especially servers and routers), of which there have been innumerable instances targeting Web-sites in the United States, Japan, South Korea and Taiwan.

Viruses have been produced that only attack Japanese-language operating systems. For example, the Win32/KillDPT 'intelligent' virus, after reading the registry keys and judging the type of operating system and determining that it uses Japanese language, will destroy the hard disc by filling it with garbage data and then restarting the system, completely paralysing the computer. Another virus which only attacked Japanese operating systems, W32.Welchia.B, was launched in 2008 and was called the 'patriotic virus' or the 'anti-Japan virus'.[19]

Second, cyber-warfare activities place a premium on 'sleeper' Trojan Horses which are installed during peacetime and which, when activated, can either damage or destroy systems, or begin to exfiltrate confidential information back to Beijing. For example, a worm called Worm.Downad.E (an advanced variant of the Conficker worm), released on 1 April 2009, and which infects Microsoft operating systems, can remain dormant in the system until a specially crafted RPC (Remote Procedure Call) request is received; its creators can then take control of the compromised computers.[20] It was reported in April 2009 that "hackers believed to be backed by the Chinese communist regime" had infiltrated computers critical to the functioning of the US electric power grid and deposited software that would allow them to "catastrophically disrupt service" when ordered.[21]

On 17 November 2008, the US Department of Defense (DoD) banned USB storage devices across the whole US military. The ban on portable digital media was imposed throughout the Defense Department's Global

[19] Zhang Dongfeng, 'Can a Computer Virus be "Patriotic?"', *China Digital Times*, 6 April 2011, <http://chinadigitaltimes.net/2007/10/can-a-computer-virus-be-patriotic-zhang-dongfeng/> [Accessed 18 May 2011].

[20] Joshua Philipp, 'Conficker Computer Virus Poses New Threat', *The Epoch Times*, 10 April 2009, <http://www.theepochtimes.com/n2/content/view/15101/> [Accessed 18 May 2011], p. A4; and Phillip Porras, Hassen Saidi and Vinod Yegneswaran, 'An Analysis of Conficker's Logic and Rendezvous Points', SRI International Technical Report, Menlo Park, California, 4 February 2009, <http://mtc.sri.com/Conficker/> [Accessed 18 May 2011].

[21] Suman Srinivasan, 'Chinese Hackers Penetrate U.S. Electric Power Grid', *The Epoch Times*, 10 April 2009, <http://www.theepochtimes.com/n2/content/view/15058/> [Accessed 18 May 2011], pp. A1, A4.

Information Grid, which includes more than 17,000 local- and regional-area networks and approximately seven million individual computers, and covered "memory sticks, thumb drives and camera flash memory cards". The ban followed reports that a worm virus known as 'Agent.btz' had been found to have infected some DoD networks. 'Agent.btz', which was believed to have originated in China, was described as:

> a variation of an older worm that copies itself to removable USB drives from infected computers and then spreads itself to whatever new systems it is connected to through USB ports.[22]

Indian computer systems and networks have also been hit by Chinese attackers. For example, India's INSAT 4B communications satellite suffered a malfunction in July 2010. It used Siemens software that was the targeted by a Stuxnet worm that apparently entered the satellite through its control system software. It has been speculated that Chinese hackers disabled the Indian satellite for commercial advantage, in an exercise of 'higher statecraft'.[23]

On 10 June 2010, South Korea claimed that a government Web-site was attacked the previous day from Internet addresses in China. The intrusions involved a Distributed Denial-of-Service attack, and were launched from 120 IP addresses. The targeted Web-site reportedly provided "information on administrative services and government policies". The attacks were similar to those made against the Web-sites of the Office of the Presidency and the Ministry of Defence in Seoul in July 2009.[24]

On 4 March 2011, South Korea's National Cyber Security Center said that about forty South Korean government and private Web-sites had been

[22] William H. McMichael and Bruce Rolfsen, 'DoD Confirms Computer Virus in Networks', *Air Force Times*, 21 November 2008, <http://www.airforcetimes.com/news/2008/11/ military_thumbdrives_computerworm_112108w/> [Accessed 18 May 2011]; Jennifer H. Svan and David Allen, 'DOD Bans the Use of Removable, Flash-type Drives on All Government Computers', *Stars and Stripes*, 21 November 2008, <http://www.stripes.com/news/ dod-bans-the-use-of-removable-flash-type-drives-on-all-government-computers-1.85514> [Accessed 18 May 2011].

[23] Jeffrey Carr, 'Did the Stuxnet Worm Kill India's INSAT-4B Satellite?', *Forbes.com*, 29 September 2010, <http://blogs.forbes.com/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/> [Accessed 18 May 2011]; Peter J. Brown, 'Lost Asian Satellites Send Powerful Signals', *Asia Times Online*, 9 October 2010, <http://www.atimes.com/atimes/ China/LJ09Ad01.html> [Accessed 18 May 2011]; Abhishek Shah, 'Was Iranian Nuclear Plant Computer Virus Made in China to Disable Indian Communications Satellite', Green World Investor, 11 October 2010, <http://greenworldinvestor.com/2010/10/11/was-iranian-nuclear-plant-computer-virus-made-in-china-to-disable-indian-communications-satellite/> [Accessed 18 May 2011].

[24] Saeromi Shin and Ben Richardson, 'South Korea Says Cyber Attacks Came From China Sites', *Bloomberg Businessweek*, 10 June 2010, <http://www.businessweek.com/news/2010-06-10/south-korea-says-cyber-attacks-came-from-china-sites-update1-.html> [Accessed 18 May 2011]; 'A Computer Attack from China Blocks South Korean Government Site', *Technology News*, 10 June 2010, <http://www.technoinfonews.info/2010/06/computer-attack-from-china-blocks-south.html> [Accessed 18 May 2011].

attacked the previous day, including those of "the presidential office, the Foreign Ministry, the National Intelligence Service, U.S. Forces Korea, and financial institutions", and that these attacks originated in China. The attacks involved a more sophisticated form of Denial-of-Service operation, in which two peer-to-peer file-sharing Web-sites were initially infected with malware, from which up to 11,000 PCs were then taken over and used in the DOS attack.[25]

Taiwan has been subjected to regular attacks on government Web-sites since the late 1990s, although these can mainly be attributed to private Netizens. However, some have undoubtedly been generated by Chinese government agencies, particularly those involving attacks on the Web-sites and networks of Taiwan's Ministry of National Defense (MND) and intelligence organisations. In July 2004, Chinese hackers attacked Web-sites of the MND in an attempt to disrupt its annual *Han Kuang-20* (Han Glory-20) defence exercise.[26] In July 2006, the Ministry included its "first-ever anti-hacker drill" in its *Han Kuang-22* exercise as "a way of raising awareness of the dangers of 'careless leaks' of classified information via the Internet".[27] The Web-site of Taiwan's National Security Bureau (NSB) was reportedly attacked from China about 590,000 times from January to October 2010, or an average of about 2000 times a day.[28]

The Taiwanese media have reported that some Chinese hackers utilise Taiwan to practice their skills. Others route their attacks through Taiwanese servers, mainly because of the common language. For example, six Internet addresses in Taiwan were used in attacks on Google in January 2010.[29]

Cyber-intelligence Operations

China is credibly reported to have conducted cyber-intelligence operations against numerous countries, including the United States, the United

[25] Clive Webster, 'South Korea Cyber-attacked', *Bit-Tech*, 4 March 2011, <http://www.bit-tech.net/news/bits/2011/03/04/south-korea-cyber-attacked/1> [Accessed 18 May 2011]; Steve Ragan, 'S. Korea Says China Targeted Global Hawk Purchase Plans', *The Tech Herald*, 8 March 2011, <http://www.thetechherald.com/article.php/201110/6913/S-Korea-says-China-targeted-Global-Hawk-purchase-plans> [Accessed 18 May 2011].
[26] 'Taiwan Shows Force on Beach Facing Chinese Mainland', *Free Republic*, 28 July 2004, <http://www.freerepublic.com/focus/f-news/1179921/posts> [Accessed 18 May 2011].
[27] Jimmy Chuang, 'Military Stages First-ever Anti-hacker Drill', *Taipei Times*, 15 July 2006, <http://www.taipeitimes.com/News/taiwan/archives/2006/07/15/2003318858> [Accessed 18 May 2011].
[28] Rich Chang, 'National Security Bureau Says that Its Computer System was Not Hacked', *Taipei Times*, 28 March 2011, <http://www.taipeitimes.com/News/taiwan/archives/2011/03/28/2003499317> [Accessed 18 May 2011].
[29] Vincent Y. Chao, 'Google Attacks Used Addresses Based in Taiwan', *Taipei Times*, 16 January 2010, <http://www.taipeitimes.com/News/front/archives/2010/01/16/2003463643> [Accessed 18 May 2011]; Ku Shu-jen, 'Chinese Hackers Practice Their Skills in Taiwan', *Commonwealth*, no. 454 (August 2010), <http://www.cw.com.tw/article/print.jsp?id=41619> [Accessed 7 April 2011].

Kingdom, Australia, New Zealand, Canada, Germany, France, the Netherlands, Portugal, Japan, South Korea, Taiwan, India, Pakistan, Iran, Thailand, the Philippines and Indonesia.

With respect to the United States, a computer security company, Solutionary, reported in March 2009 that it had detected 128 "acts of cyberagression" per minute coming from Internet addresses in China. The Department of Defense was the main target of the attacks.[30] The US Air Force estimated in 2007 that China had "successfully exfiltrated at least 10 to 20 terabytes" of sensitive data from US Government computers.[31] The amount obtained from US defence industry networks would be much greater. A State Department cable in 2008 revealed that:

> since 2002, cyber intruders involved in what is referred to as the Byzantine Candor (BC) attack, believed to originate from China, have exploited the vulnerabilities of Windows to steal log-in credentials and gain access to hundreds of US government and cleared defence contractor systems over the years.

It stated that:

> In the US, the majority of the systems BC actors have targeted belong to the US Army, but targets also include other Department of Defense services as well as Department of State, Department of Energy, additional US government entities, and commercial systems and networks.[32]

US officials involved in talks with China at the Copenhagen climate change summit in 2009 were "subject to a cyber attack containing the 'poison ivy' remote access tool intended to give hackers almost complete control over the victim's system". According to a State Department cable:

> The message had the subject line 'China and Climate Change' and was spoofed to appear as if it were from a legitimate international economics columnist at the National Journal.[33]

In November 2010, a US Congressional advisory group reported that a Chinese state-owned telecommunications company had hijacked US Internet traffic. The incident occurred on 8 April 2010 and lasted for 18 minutes, during which time traffic was re-routed by China Telecom from major US Government and military Web-sites (including those of the US Senate and the Office of the Secretary of Defense) to China, where Chinese

[30] Bill Gertz, 'China Blocks U.S. From Cyber Warfare', *Washington Times*, 12 May 2009, <http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/print/> [Accessed 18 May 2011].
[31] Krekel, 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation',, p. 51.
[32] Robert Booth, 'WikiLeaks Cables Reveal Fears Over Chinese Cyber Warfare', *The Guardian*, 4 December 2010, <http://www.guardian.co.uk/world/2010/dec/04/wikileaks-cables-china-cyber-warfare> [Accessed 18 May 2011].
[33] Ibid.

officials were able to monitor the traffic. The re-routed traffic amounted to about 15 percent of global Internet traffic.[34]

In November 2007, the Director-General of MI5 in Britain took the "unprecedented step" of openly accusing China of carrying out "state-sponsored espionage against vital parts of Britain's economy, including the computer systems of big banks and financial services firms". In a confidential letter to 300 chief executives and security chiefs at banks, accountants and legal firms, he warned them that they were under attack from "Chinese state organisations", and that "British companies doing business in China are being targeted by the Chinese Army, which is using the Internet to steal confidential commercial information", and provided "a list of known 'signatures' that can be used to identify Chinese Trojans and a list of Internet addresses known to have been used to launch attacks".[35]

With respect to Australia, it was reported in September 2007 that China had "allegedly tried to hack into highly classified government computer networks in Australia … as part of a broader international operation to glean military secrets from Western nations".[36] According to media reports in February 2008, Chinese 'cyber espionage' activities have been conducted against "key Australian Government agencies", "Chinese computer hackers have launched targeted attacks on classified Australian Government computer networks", and China was "believed to be seeking information on subjects such as military secrets and the prices Australian companies will seek for resources such as coal and iron ore". The Chinese activities reportedly prompted an official review of IT security.[37] In March 2011, it was reported that the "parliamentary computers" of a least ten Federal Ministers had been hacked into by Chinese intelligence agencies in February, including those of Prime Minister Julia Gillard, Foreign Minister Kevin Rudd and Defence Minister Stephen Smith, and that "several thousand emails may have been accessed".[38]

[34] Caroline Alphonso, 'China's "Hijacking" of U.S. Data Flow Stokes Fear of Cyberespionage', *The Globe and Mail*, 18 November 2010, <http://www.theglobeandmail.com/news/technology/chinas-hijacking-of-us-data-flow-stokes-fear-of-cyberespionage/article1805319/> [Accessed 18 May 2011].
[35] Rhys Blakely, Jonathan Richards, James Rossiter and Richard Beeston, 'MI5 Alert on China's Cyberspace Spy Threat', *The Sunday Times*, 1 December 2007, <http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece> [Accessed 18 May 2011].
[36] Patrick Walters, 'China "Hacked Australian Government Computers"', *The Australian*, 12 September 2007, <http://www.news.com.au/china-hacked-australian-government-computers/story-e6frfkp9-1111114397676> [Accessed 18 May 2011].
[37] 'Chinese Cyber Espionage "Routine" in Australia', *Canberra Times*, 11 February 2008, p. 5.
[38] Simon Benson, 'China Spies Suspected of Hacking Julia Gillard's Emails', *The Daily Telegraph*, 29 March 2011, <http://www.dailytelegraph.com.au/federal-ministers-emails-suspected-of-being-hacked/story-fn5h1vlf-1226029713668> [Accessed 18 May 2011]; Joshua Philipp, 'Chinese Cyberwar Attacks Canadian and Australian Governments', *The Epoch Times*,

It was reported in February 2007 that Chinese hackers had also attempted to penetrate "highly classified government computer networks" in New Zealand, although Prime Minister Helen Clark said that she had been assured by New Zealand's intelligence agencies that "no classified information" had been taken.[39]

In February 2011, Canadian media reported that "Chinese government hackers" had penetrated the computers of the Finance and Defense Departments and the Treasury Board in Canada in January. They reportedly "also infiltrated computers in the offices of senior government officials in a bid to steal passwords providing access to key government data". A Chinese government spokesman denied involvement by Beijing in the attacks, and stated that "the allegation that the Chinese government supports Internet hacking is groundless".[40]

With respect to Germany, China's intelligence services were accused in August 2007 of hacking into Chancellor Angela Merkel's office and three other German government ministries. Germany's domestic intelligence service, the Office for the Protection of the Constitution, reportedly discovered the hacking operation in May, and "German security officials managed to stop the theft of 160 gigabytes of data which were in the process of being siphoned off German government computers". The German press reports said that Trojan Horse programs had been "concealed in Microsoft Word documents and PowerPoint files which infected IT installations when opened", that "information was taken from German computers in this way on a daily basis by hackers based in the north-western province of Lanzhou, Canton province and Beijing", and that "German officials believe the hackers were being directed by the People's Liberation Army".[41]

In the case of France, the chief of the Network Security Agency stated in March 2011 that a cyber attack occurred in France in November-December 2010 in which around 150 computers in the Finance Ministry were penetrated and documents relating to the G-20 were accessed by sources believed to have originated in China. A further 10,000 computers had to be

30 March 2011, <http://www.theepochtimes.com/n2/china/chinese-cyberwar-attacks-canadian-and-australian-governments-53878.html> [Accessed 18 May 2011].

[39] Walters, 'China "Hacked Australian Government Computers"'.

[40] 'China Denies Canada Hacking Involvement', *C114*, 18 February 2011, <http://www.cn-c114.net/583/a581917.html> [Accessed 18 May 2011]; and Philipp, 'Chinese Cyberwar Attacks Canadian and Australian Governments'.

[41] 'Espionage Report: Merkel's China Visit Marred by Hacking Allegations', *Spiegel*, 27 August 2007, <http://www.spiegel.de/international/world/0,1518,502169,00.html> [Accessed 18 May 2011].

taken off-line in March 2011 and "inspected for traces of the Trojan Horse responsible, which was apparently introduced via an email attachment".[42]

South Korean officials claimed in March 2011 that China targeted Seoul's plans for acquisition of *Global Hawk* unmanned aerial vehicles. Chinese officials flatly denied the claims. Wang Mingzhi, a military strategist at the People's Liberation Army Air Force Command College stated that "South Korea's news is groundless".[43]

Taiwan's Ministry of National Defense announced in April 2007 that Chinese Net Force hackers had used Trojan Horses to obtain information on two particularly sensitive matters, the *Po Sheng* ('Broad Victory') project (involving cooperation with the United States on C4ISR—command, control, communications, computers, intelligence, surveillance and reconnaissance) and the *Han Kuang-23* ('Han Glory-23') defence exercise.[44] In the case of the *Han Kuang-23* material, an officer working on the exercise planning staff had taken confidential information home in his laptop in order to "do more work after hours", but his laptop was penetrated by an unidentified Chinese hacker and the information stolen. In the case of the *Po Sheng* data, it had been copied by another officer onto a USB which was later found to have contained a Trojan Horse designed to send its contents back to Beijing.[45]

In the case of India, officials said in May 2008 that over the previous one and a half years, China had "mounted almost daily attacks on Indian computer networks, both government and private". The officials said that "the Chinese are constantly scanning and mapping India's official networks", and that "this gives them a very good idea of not only the content but also of how to disable the networks or distract them during a conflict". Attacks that were "sourced to China" during the first few months of 2008 included "an attack on the NIC (National Infomatics Centre), which was aimed at the National

[42] 'Hackers Target French Finance Ministry, G-20 Plans', *Hacking Mania*, 8 March 2011, <http://hackingmania.com/Blog/hackers-target-french-finance-ministry-g-20-plans> [Accessed 18 May 2011]; Daniel Flynn and Laure Bretton, 'France's G20 Plans Targeted in Cyber Attack: Minister', *Reuters*, 7 March 2011, <http://www.reuters.com/article/2011/03/07/us-g20-france-espionage-idUSTRE72619F20110307> [Accessed 18 May 2011]; Michael Cosgrove, 'Op-Ed: The Massive Network Hacking of French Ministries and the Elysée', *Digital Journal*, 9 March 2011, <http://www.digitaljournal.com/article/304457> [Accessed 18 May 2011].
[43] Ragan, 'S. Korea Says China Targeted Global Hawk Purchase Plans'.
[44] Military News Agency of the Ministry of National Defense, 'The Ministry of National Defense Reinforces its Control on Information Security to Preclude the Leak of Information', 9 April 2007, <http://mna.gpwb.gov.tw/mnanew/internet/NewsDetail.aspx?GUID=32436> [Accessed 18 May 2011].
[45] 'Taiwan on High Alert after Military Leak', 9 April 2007, <http://newsgroups.derkeiler.com/Archive/Soc/soc.culture.taiwan/2007-04/msg00007.html> [Accessed 18 May 2011]; Jimmy Chuang, 'More Military Exercise Details Leaked', *Taipei Times*, 1 May 2007, <http://newsgroups.derkeiler.com/Archive/Soc/soc.culture.taiwan/2007-05/msg00000.html> [Accessed 18 May 2011].

Security Council", and an attack on the Ministry of External Affairs.[46] In January 2010, India's National Security Advisor, M. K. Narayanan, asserted that Chinese hackers had attempted to penetrate computers in some of India's most sensitive government officers, including his own, on 15 February 2009.[47]

Two reports issued in March 2009 documented "Chinese cyber spying against Tibetan institutions". A Canadian investigation revealed a network which it called 'GhostNet' which had infected more than 1295 hosts in 103 countries, and included "computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs". It found that Tibetan computers "were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information".[48] Bugged computers were detected "in the foreign ministries of several countries, including Iran and Indonesia, and in the embassies of India, South Korea, Taiwan, Portugal, Germany and Pakistan". Investigators tracked the virus to "a group of servers on Hainan Island", and to "other servers … based in China's Xinjiang Uyghur autonomous region, where intelligence units dealing with Tibetan independence groups are based".[49]

Chinese hackers have evidently also targeted multinational energy companies. In February 2011, for example, the computer security firm McAfee alleged that Chinese attackers had made "coordinated, covert and targeted" intrusions into the systems of five major oil and gas firms to steal proprietary information. It reported that "the hackers could be traced back to China via a server leasing company in Shandong province that hosted the malware", as well as to Beijing IP (Internet Protocol) addresses, and that the attacks, which it called Operation *Night Dragon*, "focused on financial data related to oil and gasfield exploration and bidding contracts". It also claimed that the hackers had "copied proprietary industrial processes".[50]

[46] Indrani Bagchi, 'China Mounts Cyber Attacks on Indian Sites', *The Times of India*, 5 May 2008, <http://articles.timesofindia.indiatimes.com/2008-05-05/india/27760718_1_cyber-warfare-government-networks-china> [Accessed 18 May 2011].
[47] 'China Behind Hacking of Indian Computers, Says Narayanan', *The Siasat Daily*, 18 January 2010, <http://article.wn.com/view/2010/01/18/China_behind_hacking_of_Indian_computers_says_Narayanan/> [Accessed 18 May 2011].
[48] Citizen Lab, 'Tracking GhostNet: Investigating a *Cyber Espionage* Network', *Information Warfare Monitor*, 29 March 2009, <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network> [Accessed 18 May 2011].
[49] Dan Glaister, 'China Accused Over Global Computer Spy Ring', *The Guardian*, 30 March 2009, <http://www.guardian.co.uk/world/2009/mar/30/china-dalai-lama-spying-computers> [Accessed 18 May 2011]; Shishir Nagaraja and Ross Anderson, 'The Snooping Dragon: Social-Malware Surveillance of the Tibetan Movement', University of Cambridge Technical Laboratory, Technical Report No. 746, March 2009, <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.html> [Accessed 18 May 2011].
[50] Tania Branigan, 'Chinese Hackers Targeted Energy Multinationals, Claims McAfee', *The Guardian*, 11 February 2011, <http://www.guardian.co.uk/world/2011/feb/11/chinese-hackers-targeted-energy-multinationals> [Accessed 18 May 2011].

From mid-2009 to January 2010, a cyber attack originating in China was launched against Google and more than twenty other companies. According to a diplomatic cable from the US Embassy in Beijing, a Chinese source reported that the intrusions were directed by the Politburo. The cable suggested that the hacking was part of a coordinated campaign executed by "government operatives, public security experts and Internet outlaws recruited by the Chinese government". Called Operation *Aurora*, a specific purpose of the attack on Google was reportedly to access the Gmail accounts of Chinese dissidents and human rights activists. More generally, the goal was to gain access to and potentially modify source code repositories at some twenty to thirty-four high tech, security and defence contractor companies. The attackers exploited a vulnerability in the Adobe PDF format used in Microsoft's Internet Explorer browser to open a back door, through which the intruder performed reconnaissance and gained control over the source codes.[51]

In March 2011, a Denial-of-Service attack originating in China hit the blog-publishing site WordPress, interfering with the company's three data centres in Chicago, San Antonio and Dallas. The attacks directed "multiple Gigabits per second and tens of millions of packets per second".[52] And in April, an on-line petitioning platform, Change.org, which had hosted a petition urging Chinese authorities to release artist Ai Weiwei from custody, was also hit by a Denial-of-Service attack coming from China.[53]

Chinese intelligence agencies also monitor the computer files and e-mails of selected individuals. Monitoring the personal e-mails of officials can provide information that can be used for blackmail or coercion, such as a person's interest in money or sex.

China's Netizens

By 2001, when China had some 60 million Internet users (the second largest number after the United States),[54] it already had the largest number of active

[51] Bobbie Johnson, 'Chinese Hackers Used Microsoft Browser to Launch Google Strike', *The Guardian*, 15 January 2010, <http://www.guardian.co.uk/technology/2010/jan/15/microsoft-china-google> [Accessed 18 May 2011]; 'Operation Aurora', *Wikipedia*, <http://en.wikipedia.org/wiki/Operation_Aurora> [Accessed 18 May 2011]; Marzieh Ghiasi, 'Google vs. China: Cyberwarfare in a Brave New World', 13 January 2010, <http://ghiasi.org/2010/01/google-vs-china-cyberwarfare-in-a-brave-new-world/> [Accessed 18 May 2011]; Jim Finkle, 'Google China Hackers Stole Source Code', *Chinh's News*, 4 March 2010, <http://chinhdangvu.blogspot.com/2010/03/google-china-hackers-stole-source-code.html> [Accessed 18 May 2011].
[52] Michael Kan, 'WordPress: DDOS Attacks Came From China', *PCWorld*, 7 March 2011, <http://www.pcworld.com/businesscenter/article/221467/wordpress_ddos_attacks_came_from_china.html> [Accessed 18 May 2011].
[53] Ibid.
[54] 'U.S. Has 33% Share of Internet Users Worldwide Year-end 2000', *Computer Industry Almanac Inc*., Press Release, 24 April 2001, <http://www.c-i-a.com/pr0401.htm> [Accessed 18 May 2011]; 'China Climbs to Second Spot With 59m Net Users', *The Nation* (Bangkok), 20 January 2003, p. 9A.

non-governmental cyber-warriors in Asia. It surpassed the United States in Internet users in mid-2008, when it reached an estimated 253 million.[55] It reached 457 million by the end of 2010, an increase of 19 percent (or 73 million users) over 2009. Its Internet penetration rate of 34.3 percent is still relatively low compared to that of developed countries, although it is higher than the world average.[56]

Many of these non-governmental cyber-warriors are motivated by nationalist causes. Attacks on Taiwanese Web-sites began in 1996, when Chinese hackers defaced and damaged Web-sites during the Presidential election.[57] In August 1999, there was a spate of cross-Strait attacks against computer networks and official Web-sites in Taiwan, which were launched by Netizens reacting to then-President Lee Tung-hui's statement in June that relations between the PRC and Taiwan should be characterised as "special State-to-State" relations. These attacks involved more than 160 penetrations into Taiwanese computer networks. The hackers even invaded the Web-site of the American Institute in Taiwan, the unofficial US Embassy (and the location of the National Security Agency's Liaison Office in Taipei), and crashed its server with a bombardment of 45,000 simultaneous e-mails.[58] In another spate, between November 2001 and July 2002, "hackers based in China broke into 216 computers at 42 government institutions via a back-up computer processing unit at Chungwa Telecom", in what Taiwanese telecommunications officials said was "the most systematic and large-scale hijacker break-in of its kind in Taiwan".[59] In June 2004, Chinese hackers attacked the site of Taiwan President Chen Shui-bian's pro-independence Democratic Progressive Party.[60]

In January 2000, there was an intense spate of attacks on Japanese government Web-sites, probably triggered by denials by right-wing Japanese that Japanese troops had massacred Chinese civilians when they seized Nanjing in 1937. The Web-sites of at least twenty government departments were attacked, including those of the Japan Defense Agency (JDA) and the Foreign Ministry. On some sites, the hackers posted slogans criticising

[55] David Barboza, 'China Surpasses U.S. in Number of Internet Users', *New York Times*, 26 July 2008.
[56] Michael Kan, 'China's Internet Users Reach 457 Million', *PCWorld*, 19 January 2011, <http://www.pcworld.com/businesscenter/article/216979/chinas_internet_users_reach_457_million.html> [Accessed 18 May 2011].
[57] Elizabeth Becker, 'F.B.I. Warns That Chinese May Disrupt U.S. Web Sites', *New York Times*, 28 April 2001.
[58] Damon Bristow, 'Cyber-Warfare Rages Across Taiwan Strait', *Jane's Intelligence Review*, February 2000, pp. 40-1.
[59] 'Taiwan Not Helping Falun Gong Hack Into China TV Signals: Official', *Taiwan Headlines*, 26 September 2002, <http://www.taiwanheadlines.gov.tw/20020926/20020926s1.html> [Accessed 7 April 2011]; 'Taiwan Downplays China TV Hacking', *CNN.Com*, 26 September 2002, <http://asia.cnn.com/ 2002/WORLD/asiapcf/east/09/25/taiwan. Falungong/> [Accessed 18 May 2011].
[60] 'Taiwan Shows Force on Beach Facing Chinese Mainland', *Free Republic*, 28 July 2004, <http://www.freerepublic.com/focus/f-news/1179921/posts> [Accessed 18 May 2011].

Japan's war-time acts; important data was erased from one site. Twelve of the attacks were routed through ISPs (internet service providers) in the PRC, but some had probably also come through ISPs in South Korea, where there is also widespread resentment at Japan's past militarism.[61]

Another round of coordinated assaults on Japanese Web-sites occurred in early 2005, when Japan's Education Ministry approved new textbooks that critics argued 'whitewashed' the history of Japanese aggression in the region. Web-sites of the Japanese Embassy in Beijing, the National Police Agency, the Self-Defense Forces and the Defense and Foreign ministries were repeatedly taken down by Denial-of-Service attacks. The servers for the Web-site for Tokyo's Yasukuni Shrine were clogged by millions of 'ping' strikes.[62] And in September 2010, when tensions between China and Japan increased amid the territorial dispute over the Senkaku (or Diaoyu) Islands in the East China Sea, the Web-sites of both the Defense Ministry and the National Police Agency were bombarded in Denial-of-Service attacks by Chinese hackers.[63]

During the NATO air war against Yugoslavia in March-June 1999, Chinese hackers attacked hundreds of government and military Web-sites and other information systems in the United States, the United Kingdom, and other NATO countries. 'Ping' attacks were launched to crash NATO Web servers. The attacks became especially virulent following the US bombing of the Chinese Embassy in Belgrade on 7 May. In the United States, computer systems at the White House, the Pentagon and the State Department were attacked. More than 100 government Web-sites in the United States received virus-infected e-mails. Hackers also penetrated the Web-site of the US Embassy in Beijing.[64] In May 2001, in the aftermath of the EP-3E incident (and the second anniversary of the US bombing of the Chinese Embassy in Belgrade), Chinese hackers attacked "a few hundred" US Web-sites.[65] The official White House home page suffered a Denial-of-Service attack for more than two hours on 4 May.[66]

[61] 'Japan Crime: Cyber-terror Task Force Established', *Bangkok Post*, 27 January 2000, p. 6; Chester Dawson, 'Cyber Attack', *Far Eastern Economic Review*, 10 February 2000, p. 21.
[62] Anthony Faiola, 'Cyber Warfare: China vs Japan', 11 May 2005, <http://www.crime-research.org/news/11.05.2005/1227/> [Accessed 18 May 2011].
[63] 'Japan Suspects Cyber Attacks Amid China Row: Media', *Space Daily*, 17 September 2010, <http://www.spacedaily.com/reports/Japan_suspects_cyber_attacks_amid_China_row_media_999.html> [Accessed 18 May 2011].
[64] John Parker, *Total Surveillance: Investigating the Big Brother World of E-Spies, Eavesdroppers and CCTV* (London: Piatkus, 2000), p. 280; Bill Gertz, 'Chinese Hackers Raid U.S. Computers', *The Washington Times*, 16 May 1999.
[65] Ron Chepesiuk, 'Get Ready for Cyberwars', *New California Media*, 23 August 2001, <http://www.ncmonline.com/content/ncm/2001/aug/0823cyberwars.html> [Accessed 7 April 2011].
[66] 'White House Website Attacked', Cosmiverse.com, 7 May 2001, <http://www.cosmiverse.com/tech05070102.html> [Accessed 18 May 2011].

In September 2002, it was reported that since late April Chinese hackers had been trying to penetrate the Dalai Lama's computer network. The manager of the Tibetan Computer Resource Centre in Dharamsala, in India, said that "Chinese hackers had designed a virus to plug into the network and steal information".[67] The attacks came in hundreds of e-mails using false addresses appearing to be friendly sources, and included Trojan Horse programs designed to seek out files and attempt to e-mail them to an address in China, and programs designed to open 'back doors' to allow the hackers to take control of target computers through Internet connections. According to dissident groups, who were sometimes able to trace the source of the attacks, the hacking was officially sponsored: "They are Chinese hackers employed by a State-owned industry operating on the State's time".[68]

There is no doubt that the Chinese authorities exercise some degree of control over some of these hackers. In May 2002, for example, when the US Department of Defense reportedly braced itself for an onslaught of cyber attacks, they never materialised because (according to the Deputy Commander of the Pentagon's Joint Task Force on Computer Network Operations), "actually the government of China asked them not to do that".[69]

It was reported in November 2008 that the largest US military base in Afghanistan, at Bagram, was hit by a computer virus that affected nearly three-quarters of the computers on the base. This was not the first such cyber-attack. Officials stated that "earlier incarnations of the virus had exported information such as convoy and troop movements". It could not be determined "whether the viruses were part of a covert Chinese government effort or the work of private hackers", although US military spokesmen did say that the Chinese "learn a lot from these attacks, like how our logistics and other systems work".[70]

In a secret cable in June 2009, the US State Department noted that Chinese authorities were working with private companies that were known to have recruited infamous hackers. It stated that "there is a strong possibility the PRC is harvesting the talents of its private sector in order to bolster offensive and defensive computer network operations capabilities", warned that the "potential linkages of China's top companies with the PRC illustrate the government's use of its private sector in support of information warfare

[67] Bodeen, 'Mainland Asks Taiwan to Stop Interference'.
[68] Doug Nairne, 'State Hackers Spying On Us, Say Chinese Dissidents', *South China Morning Post*, 18 September 2002.
[69] Cited in Pamela Hess, 'China Prevented Repeat Cyber Attack on US', InfoSecNews.org, 29 October 2002, <http://www.infosecnews.org/hypermail/0210/6714.html> [Accessed 18 May 2011].
[70] Anna Mulrine, 'Computer Virus Hits U.S. Military Base in Afghanistan', *U.S. News and World Report*, 28 November 2008, <http://www.usnews.com/news/iraq/articles/2008/11/28/computer-virus-hits-us-military-base-in-afghanistan> [Accessed 18 May 2011].

objectives", and gave two examples of hacker recruitment. One was Lin Yong (also known as 'LION'), who founded the Honkers Union of China (HUC) which attacked US and Japanese networks around 2001, and the other was the XFocus group which produced the Blaster worm in 2003.[71]

In July 2008, CNN reporters met with members of a hacking group that operated from an apartment on the island of Zhoushan, just south of Shanghai, and who claimed that they had "hacked into the Pentagon and downloaded information". They also claimed that they had been "paid by the Chinese government".[72]

Pentagon officials told a Congressional hearing in Washington in March 2008 that computer networks in the United States, Germany, Britain and France had been hit by "multiple intrusions" originating from China during 2007, but were generally cautious about attributing these to the Chinese military or government authorities as opposed to private Netizens. However, David Sedney, the Deputy Assistant Secretary of Defense for East Asia, testified that: "The way these intrusions are conducted are certainly consistent with what you would need if you were going to actually carry out cyber warfare".[73]

On the other hand, several factors militate against the PLA's incorporation of Netizen or 'hacktivist' activities in its plans for computer network operations in war-time. Guiding and directing these activities would be very difficult. Hacktivist activities have the potential to interfere with and "inadvertently disrupt" the PLA's own attacks. They also:

> risk shutting down the lines of communication in use for intelligence collection or accidentally overwhelm channels the PLA is using as feedback loops to monitor the effectiveness of [its] network attacks.[74]

China's Vulnerabilities

Chinese officials have pointed out that "China is the biggest victim country of hacking".[75] Official data showed that "more than one million IP addresses were under control by overseas sources", and that more than 42,000 Web-sites were "tampered by hackers" in 2009.[76] According to the National

[71] Booth, 'WikiLeaks Cables Reveal Fears Over Chinese Cyber Warfare'.
[72] John Vause, 'Red Chinese Hackers: No Site is Safe', *CNN.com*, 11 March 2008, <http://edition.cnn.com/2008/TECH/03/07/china.hackers/index.html> [Accessed 18 May 2011].
[73] Julian E. Barnes, 'Chinese Hacking Worries Pentagon', *Los Angeles Times*, 4 March 2008, <http://articles.latimes.com/2008/mar/04/world/fg-uschina4> [Accessed 18 May 2011]; Vause, 'Red Chinese Hackers: No Site is Safe'.
[74] Bryan Krekel, 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation', p. 40.
[75] 'Accusation of Chinese Government's Participation in Cyber Attack "Groundless": Ministry', *Xinhua*, 25 January 2010, <http://news.xinhuanet.com/english2010/china/2010-01/25/c_13149276.htm> [Accessed 18 May 2011].
[76] Ibid.

Computer Network Emergency Response Technical Coordination Centre in Beijing in a report released in March 2011, more than 4600 Chinese government Web-sites had their content modified by hackers in 2010, an increase of 68 percent over the previous year.[77]

A two-month survey conducted in mid-2003 by officials of the Ministry of Public Security showed that 85 percent of computers in China were infected with a computer virus. The officials noted that "the main reason for the spread of the viruses was increasing use of the internet and e-mail".[78] The proportion increased to 88 percent in 2004, but then dropped to about 80 percent in 2005.[79] A Chinese Internet security company reported in July 2007 that more than 35 million computers in China had been attacked by viruses in the first half of that year. It estimated that 68.71 percent of the viruses were Trojan Horses, of which 76.04 percent were "phishing-related viruses".[80] A study covering January-November 2008 found that the number infected had increased by 12.16 percent compared to the previous year, and that 64 percent were Trojans, 20 percent back door viruses, 12 percent other viruses and four percent worms. The majority were being used by hackers to steal virtual property.[81]

A list of the top 100 viruses infecting computers world-wide at the beginning of 2011 showed that in every single case China was the country "most affected".[82] Moreover, nearly all these viruses originated in China. The top 10 in 2008 all originated in China: Trojan.PSW.Win32.GameOL, which opens up firewalls and collects confidential information such as personal financial information; Trojan.Win32.Undef, similar to PSW.Win32.GameOL; RootKit.Win32.Mnless, which obtains root privileges and uses them to modify the operating system, extract passwords and other confidential information, and, if so directed, destroy the host computer; Hack.Exploit.Swf, first detected in July 2008, which is transmitted from infected Web-sites and which affects Windows NT, 2000, XP and 2003; Trojan.PSW.SunOnline, a Trojan which installs itself on PCs and destroys data and files on those PCs;

[77] Mark Lee, 'China Reports 68% Jump in Cyber Attacks on Government Websites', *Bloomberg*, 10 March 2011, <http://www.bloomberg.com/news/2011-03-10/china-reports-68-jump-in-hacking-attacks-on-government-websites-in-2010.html> [Accessed 18 May 2011].
[78] 'Computer Viruses Rampant in China', *BBC News*, 21 October 2003, <http://news.bbc.co.uk/2/hi/technology/3210086.stm> [Accessed 18 May 2011].
[79] 'Computer Virus Infection Rate Down in China', Icrontic, 18 November 2005, <http://icrontic.com/forum/showthread.php?t=39565> [Accessed 18 May 2011].
[80] 'Report: China Suffers Most From Computer Viruses', China Tech News.com, 30 July 2007, <http://www.chinatechnews.com/2007/07/30/5691-report-china-suffers-the-most-from-computer-virus> [Accessed 18 May 2011]; 'Kingsoft Releases Computer Virus Security Report', China Tech News.com, 6 July 2007, <http://www.chinatechnews.com/2007/07/06/5605-kingsoft-releases-computer-virus-security-report> [Accessed 18 May 2011].
[81] Heike, 'China's Computer Virus Epidemic Shows 12% Increase', *The Dark Visitor*, 18 November 2008, <http://www.thedarkvisitor.com/2008/11/chinas-computer-virus-epidemic-shows-12-increase/> [Accessed 18 May 2011].
[82] 'Top 100 Virus Threats', PC1News.com, <http://www.pc1news.com/virus/top100.html> [Accessed 18 May 2011].

RootKit.Win32.Undef, which is similar to RootKit.Win32.Mnless; Trojan.PSW.Win32.XYOnline, which is similar to the first two viruses; Trojan.Clicker.Win32.Pophot, also similar; Worm.Win32.Agent, released on 6 July 2006, which affects the Windows PE EXE file; and Trojan.PSW.Win32.QQPass, released on 24 September 2006, which also affects the Windows PE EXE file and which is designed to steal user passwords.[83]

According to Chinese sources, China has over thirty active Internet virus groups. Ten virus-producing groups account for 80 percent of viruses in the country: these are known as the Huangfei Hu, HYC, HY, Old Serpent, 192, GZWZ, CL, Zhang Feng, WG, and Anne Groups.[84] These virus groups differ from hackers in that they do not directly steal money. Rather, they use a variety of techniques to re-direct computer users to selected Web-sites, including "tampering with pop-up advertisements, creating website links on people's desktops, changing the computer's homepage or changing icons on the bookmarks bar". A Chinese cyber security expert has noted that:

> it is extremely difficult to destroy these groups. The virus group Huangfeihu, for example, changed its IP address over 500 times within one year and is vigilant to the extreme. But what's even more key in the situation is that many of these groups set up their servers abroad, hence making them impossible to trace.[85]

The Chinese regime has attempted to impose greater control over internal networks, both to suppress domestic opposition and to block penetration from outside the country. It has surrounded the country with a Great Firewall, also referred as the Golden Shield Project, which is an Internet censorship and surveillance project operated by the Ministry of Public Security (MPS). It was initiated in 1998, following approval by the State Council of the 'Computer Information Network and Internet Security, Protection, and Management Regulations' on 11 December 1997, when Internet usage was becoming popular in China, and took operational effect in November 2003. It is estimated that between 30,000 and 50,000 Internet police are employed in this project.[86] New laws were enacted in April 2010 which require Internet and mobile phone operators "to inform the authorities

[83] Heike, 'China's Computer Virus Epidemic Shows 12% Increase'. See also Kaspersky.com, 'Virus Watch', <http://www. kaspersky.com/viruswatchlite?search_virus=Trojan-Downloader.Win32.Bagle&hour_offset =6&x=15&y=7> [Accessed 18 May 2011].
[84] 'China's Top Ten Virus Secret Groups Exposed and Their Five Means of Illegal Profits', 6 March 2011, <http://www.pcwarn.com/chinas-top-ten-virus-exposure-secret-group-means-of-the-five-illegal-profits/> [Accessed 18 May 2011].
[85] 'Computer Viruses: A Highly Lucrative Market in China', eChinacities.com, 6 March 2011, <http://www.echinacities.com/china-media/why-computer-viruses-are-a-highly-lucrative-market-in-china.html> [Accessed 18 May 2011].
[86] Amnesty International, 'What is Internet Censorship?', 28 March 2008, <http://www.amnesty.org.au/china/comments/10926/> [Accessed 18 May 2011].

of any illegal information being transmitted on their systems", i.e., any information that might affect political stability.[87]

Since the beginning of the 2000s, Beijing has been pushing both government agencies and the business sector to use Unix and Linux operating systems. More recently, it has mandated the use of *Kylin*, a highly secure, Unix-based operating system, apparently much more secure than Microsoft server software, which China's University of Science and Technology for National Defence developed, and installation of which began on government and military systems in 2009, with the intention of making Beijing's networks "impenetrable to U.S. military and intelligence agencies".[88]

It is clear that there are at least as many Netizens concerned with breaching the Great Firewall (a practice known as *fanqiang*, or '*s*caling the wall') as there are with attacking foreign networks.[89] Several techniques are used which evade blocking by using third party sites that are not filtered, including VPN (virtual private network) services, such as GPass or Hotspot Shield; blocking-resistant tools, such as Freegate or Ultrasurf; secure shell (SSH) access tools; proxy servers; and anonymity software such as Tor, which is also an effective circumvention tool.[90]

James Lewis, the cyber-warfare expert at the Center for Strategic and International Studies (CSIS) in Washington, D.C., has argued that Beijing's need to secure China's computers and networks against internal dissent and opposition actually comprises an 'asymmetric handicap'. He has pointed out that: "For all the effort the Chinese put into cyber competition, external efforts"—against a potential foe like the United States—"are second priority. The primary priority is domestic control and regime survival. The external part is a side benefit".[91]

---

[87] Nigel Inkster, 'China in Cyberspace', *Survival*, vol. 52, no. 4 (August-September 2010), pp. 55-66.

[88] Gertz, 'China Blocks U.S. From Cyber Warfare'; 'China Turns Unix Into a Weapon', *Strategy Page*, 14 May 2009, <http://www.strategypage.com/htmw/htiw/articles/20090514.aspx> [Accessed 18 May 2011].

[89] Aida Shelton, 'Scaling the Firewall: How Chinese Netizens Take the Internet Into Their Own Hands', eChinacities.com, 23 September 2010, <http://www.echinacities.com/expat-corner/scaling-the-firewall-how-chinese-netizens-take-the.html> [Accessed 18 May 2011].

[90] Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris and John Palfrey, '2010 Circumvention Tool Usage Report', The Berkman Center for Internet & Society, Harvard University, October 2010, <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf> [Accessed 18 May 2011]; Chen Chen, 'Netizens Bypassing the Great China Firewall', China Decoded, 26 July 2010, <http://www.chinadecoded.com/2010/07/26/netizens-bypassing-the-great-china-firewall/> [Accessed 18 May 2011].

[91] Cited in James Fallows, 'Cyber Warriors', *The Atlantic*, March 2010, <http://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/7917/2/> [Accessed 18 May 2011]. See also James A. Lewis, 'The Architecture of Control: Internet Surveillance in China', Center for Strategic and International Studies, Washington, D.C., July 2006, <http://csis.org/files/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf> [Accessed 18 May 2011].

Conclusions

Chinese strategists are quite aware of their own deficiencies and vulnerabilities with respect to cyber-warfare. In June 2000, "a series of high-technology combat exercises" being conducted by the PLA "had to be suspended" when they were attacked by "a computer hacker".[92] China's telecommunications technicians were impotent against the intermittent hijacking of the Sinosat-1 national communications satellite by Falun Gong 'practitioners' in the early 2000s. China's demonstrated offensive cyber-warfare capabilities are fairly rudimentary. Chinese hackers have been able to easily orchestrate sufficient simultaneous 'pings' to crash selected Web servers (i.e., Denial-of-Service attacks). They have been able to penetrate Web-sites and deface them, erase data from them, and post different information on them (such as propaganda slogans). And they have developed various fairly simple viruses for spreading by e-mails to disable targeted computer systems, as well as Trojan Horse programs insertible by e-mails to steal information from them. However, they have evinced little proficiency with more sophisticated hacking techniques. The viruses and Trojan Horses they have used have been fairly easy to detect and remove before any damage has been done or data stolen. There is no evidence that China's cyber-warriors can penetrate highly secure networks or covertly steal or falsify critical data. They would be unable to systematically cripple selected command and control, air defence and intelligence networks and databases of advanced adversaries, or to conduct deception operations by secretly manipulating the data in these networks. The gap between the sophistication of the anti-virus and network security programs available to China's cyber-warriors as compared to those of their counterparts in the more open, advanced IT societies, is immense. China's cyber-warfare authorities must despair at the breadth and depth of modern digital information and communications systems and technical expertise available to their adversaries.

China is condemned to inferiority in IW capabilities for probably several decades. At best, it can employ asymmetric strategies designed to exploit the (perhaps relatively greater) dependence on IT by their potential adversaries—both the C^3ISREW elements of adversary military forces and the vital telecommunications and computer systems in the adversary's homelands. In particular, attacks on US information systems relating to military command and control, transportation and logistics could "possibly degrade or delay U.S. force mobilisation in a time-dependent scenario", such as US intervention in a military conflict in the Taiwan Straits.[93] China's cyber-warfare capabilities are very destructive, but could not compete in

[92] 'Asian Infowar: The Top Ten', *Jane's Foreign Report*, No. 2617 (16 November 2000), p. 5; Damon Bristow, 'Asia: Grasping Information Warfare?', *Jane's Intelligence Review*, December 2000, p. 33.
[93] Mulvenon, 'The PLA and Information Warfare', pp. 175, 176, 184-5.

extended scenarios of sophisticated IW operations. In other words, they function best when used pre-emptively, as the PLA now practices in its exercises.[94] In sum, the extensive Chinese IW capabilities, and the possibilities for asymmetric strategies, are only potent if employed first.

Table 1: Selected Chinese Computer Virus and Worm Designs

AntiCMOS	Typical boot sector virus, infects master boot sectors on hard disks and boot sectors on diskettes. Stays resident in memory. Originated in Hong Kong in 1994.
Changsha	Simple non-resident virus for overwriting COM/EXE files. 3072 bytes.
Dalian	Also called Gene. Stays resident in memory and infects EXE files when they are listed with the DIR command. 1366 bytes. Produced in China in July 1997.
Deloder	Network worm which infects Windows machines with weak passwords to the Administrator account. Installs VNC [Virtual Network Computer] remote access server and IRC [Internet Relay Chat] backdoor files. 745,984 bytes. Found 9 March 2003.
Democracy	Resident COM/EXE-files virus, contains the text: 'Democracy'. 3806 bytes.
Little Red	Also called Mao. Resident COM/EXE-files. Activated on 26 December or 9 September, the birth and death dates of Mao Tse-tung, playing Chinese songs from the PC speaker. 1465 bytes. Common in 1994-95.
Mange-tout	Resident COM/EXE-files virus. 1099 bytes. 1994.
Quartz	Infects EXE files and tries to disable the serial port of the machine. 1345 bytes.
Welcomb	Common boot sector virus containing the text: 'Welcome to BUPT 9146, Beijing!'
Lion	Affected LINUX operating systems. Created by 'LION', founder of the hacker group called the Honkers Union of China (HUC). Created to protest Japanese textbooks that said the Japanese occupation of China and Korea was justified and beneficial to the occupied countries. Infected LINUX machines through TSIG [Transaction Signature] vulnerabilities in BIND [Berkeley Internet Name Domain] DNS [Domain Name System] servers. Installed hacker toolkit called 'tOrn rootkit', as well as Trojan horses. Passwords and network information sent to huckit@china.com, liOnip@china.com, liOnsniffer@china.com, and liOnkit@china.com. March-April 2001.
Adore	Also called the 'Red Worm'. Affected LINUX operating systems. Variant of LION. Password and system configuration files e-mailed to two addresses in China (adore9000@china.com and adore9001@china.com). Created by the HUC group in retaliation for the death of a Chinese fighter pilot in a collision with a US EP-3E aircraft near Hainan Island on 1 April 2001.

[94] Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2007*, p. 22.

Code Red	Infected machines using Microsoft IIS [Internet Information Services] Web server software, exploiting 'buffer overflow' vulnerability. Combined defacement of Web sites with DDOS [Distributed Denial-of-Service] attacks. White House Website bombarded on 19 July 2001. More than a million servers infected world-wide. Caused US$2.6 billion damage. Originated at a computer at the University of Foshan in Guandong. The Code Red II worm, a complete re-write of Code Red, was released on 4 August 2001.
Nimda	(Admin backwards). Also called W32/Nimda.A-mm. Mass-mailing and network worm that infected both PC Windows and Microsoft IIS Web servers. Could infiltrate LANs and create user accounts with access to files and e-mail. Developed by same authors as Code Red. September 2001.
Lovgate	Also called Supnot. A mass-mailing and network worm. Has a backdoor component allowing the attacker to perform designated actions on the infected machine. The worm has its own SMTP [Simple Mail Transfer Protocol] engine and connects the host to two addresses at a Chinese Web portal (163.com). March-June 2003.
Blaster	Worm produced by XFocus, and released in August 2003. Infected computers using Windows XP and Windows 2000.
Xiongmao Shaoxiang	'Panda Burning Joss Sticks'. Began spreading through the Internet in December 2006. Steals the account names and passwords of on-line game players and popular chat sites. Described as "the worst computer virus" in China in 2006.
Hao	Attaches itself to all .exe files. 'More vicious' than Xiongmao Shaoxiang. Appeared in August 2007.
Mocmex	Recognises and blocks anti-virus protection software. The first computer virus on a digital photo frame. First detected on 17 February 2008.
Wecorl	Found in August 2008. Uses a worm to infect peer systems and load Distributed Denial-of-Service programs.
W32.Welchia.B	Appeared in 2008. Only attacked Japanese-language operating systems. Called the 'patriotic virus' or the 'anti-Japan virus'.
Agent.btz	A worm that copies itself to removable USB drives from infected computers and then spreads itself to whatever new systems it is connected to through USB ports. Discovered in US DoD networks in November 2008.
Conficker	First detected on 21 November 2008. Five main variants, A (21 November 2008), B (29 December 2008), C (20 February 2009), D (4 March 2009) and E (7 April 2009). Closely related to Nimda. Infected from 9 to 15 million Microsoft server systems running everything from Windows 2000 to the Windows 7 Beta.
Worm_Downad.E	An update of Conficker, also known as W32/Confick-D (Sophos). Initiated on 1 April 2009. Infects Microsoft operating systems, and remains dormant in the system until a specially crafted RPC (Remote Procedure Call) request is received.
Win32/KillDPT	Appeared in early 2011. Only attacks Japanese-language operating systems.

Desmond Ball is a Professor in the Strategic and Defence Studies Centre at the Australian National University, Canberra. He was Head of the Centre from 1984 to 1991. desmond.ball@anu.edu.au.