THE INTERNET IN CHINA: CIVILIAN AND MILITARY USES

Timothy THOMAS

Introduction

During the past five years China has developed an impressive telecommunications industry with the potential to become the world's largest communications market. At the end of the year 2000, there were 22 million Internet users, while projections for the year 2005 estimate 130 million users. Optical fiber now joins the capitals of all of China's provinces and its 1.3 billion people together, providing the integrating factor for such growth in users.

Of equal importance is how the Chinese government plans to utilize the Internet for military purposes. According to Chinese information warfare specialist Shen Weiguang, the Internet can be used to implement Chinese strategies to destroy or deface private and official web sites. Shen wrote in his book *The Third World War—Total Information War* that the Shenyang Military region organized

> "… military exercises in IW [Information Warfare] using live soldiers … On the computer, people have come up with 36 ways to disrupt the Internet and 36 ways to defend against such disruption. There are also proposals to create a social order for the future information world."[1]

According to Shen every computer chip is a potential weapon, every computer may become an effective fighting platform, and every citizen may develop a war plan and use the Internet to launch a special war. Internet war is a part of peacetime IW in Shen's view, making the purpose of war "controlling the enemy and preserving oneself" through Internet confrontations and online military exercises. Shen also noted that the Internet is a "New World" with no border and no treaties.[2]

This article addresses three aspects of the civilian and military use of China's Internet. First, it looks at Internet use by China's citizens, and the information

INFORMATION & SECURITY. An International Journal, Vol. 7, 2001, 159-173.

technologies that support it. This includes an examination of the role of President Jiang Zemin's son in this process. Second, it examines how the military has implemented the Internet into its operations, both as a mobilizer of People's Liberation Army (PLA) emotions and as a provider of news, and as a new tool for political officers. Finally, the article looks at three recent Internet skirmishes—China versus NATO in April and May of 1999, China versus Taiwan in August and September of 1999, and China versus the United States in April of 2001, the latter the Chinese response to the April 1 collision of a US Navy surveillance and reconnaissance plane and a Chinese fighter.

1. The Internet in China

Over the past few years, use of the Internet has skyrocketed in Mainland China. While a February 2000 *Jane's Intelligence Review* article on China and Taiwan stated that China had 4 million Internet users, a survey for Greater China (China, Hong Kong, and Taiwan) in the fourth quarter of 2000 conducted by the online research company Interactive Audience Measurement Asia (Iamasia) found that there were 15.2 million Internet users in China, 2.2 million in Hong Kong, and 6.4 million in Taiwan. In the classroom, "Iamasia" noted Taiwan has 40% of its students using school facilities to go online, while only 21% do so in Hong Kong and only 8% in China.[3]

The web site Muzi.com noted in early 2001 that according to the China Internet Network Information Center (CNNIC) Internet users reached 22.5 million at the end of 2000, up from 8.9 million at the end of 1999 (when the *Jane's* article mentioned above was probably written).[4] The Internet service ChinaOnline considers these numbers dubious since CNNIC counts all regular users, not just online consumers. CNNIC is a semiofficial nonprofit organization that is run by the Chinese Academy of Sciences and handles Internet issues within the purview of the Ministry of Information Industry (MII). The Center manages and oversees English and Chinese character domain names ending in ".cn". It also maintains a database of Internet protocol addresses, provides information on Internet-related policies, and conducts surveys on Internet development, among other jobs. The center estimates that there are now 122,099 domain names registered under ".cn" and 265,405 websites in China.

According to one survey, Sina.com was listed by 68.1 % of netizens (a Web surfer who spends no less than two hours online during a session and surfs no less than twice a week) as the most influential Web site in China, followed by Sohu.com with 53.3 %, Net Ease with 40.7 %, and Chinese Yahoo! with 16 %.[5] However, when using e-mail, most users preferred Sina followed by NetEase. When searching, 60.3 % like Sohu and 54.7 % preferred Sina.[6]

Finally, the journal *Red Herring*, in its special Asia issue of October 2000, was even more optimistic. It listed Internet use in China, by the year 2005, as nearing 9.2 % of the population. This would put the Internet use figure somewhere around 125 million people.[7] Even if these figures are off by millions of people, the underlying idea is clear—the utilization of the net is widening quickly. For example, the US Embassy in China, on a web site article on "The Growing Influence of the Internet in China," noted that the Feiyu Net Café (www.feiyu.com.cn) near Beijing University has one thousand computers.

Even the government has pushed to go "on-line." As Nina Hachigian noted in *Foreign Affairs*, the "Government On-Line Initiative," launched in 1998, aimed to ensure that 80 % of all government agencies—local and national—had Web sites by the end of 2000. State-owned China Telecom lowered its access charges and is adding two million new lines each month to meet demand for network access. Other state-owned telecommunication providers are encouraged to build their own networks.[8]

Beijing-based telecoms consultancy BDA stated that 69 million people in China would access the Internet over their phones by the end of 2000, and there will be 236 million wireless subscribers and 120 million Internet users by 2004. China Mobile, China's largest mobile phone operator, said it would charge fees for wireless application protocol (WAP) services.[9] In March of 2000 it was announced that China would link four backbone Internet networks. These four are CSTNET (China Science and Technology Network), ChinaNET, CERNET (China Education and Research Network), and ChinaGBN (China Golden Bridge Network). Circuit capacity was not listed, however.

ChinaNET is a public network that connected to the Internet in early 1995. It now covers all of China's provinces and autonomous regions, and all municipalities under the central government. It has monopolized the market. CSTNET is a national Internet network constructed by Tsinghua University and Peking University. It launched its Internet access service in 1994. It networked 100 institutes by 1995, and by 1998 had connected more than 100 Ethernets, 3,000 computers and 10,000 users. CERNET began in 1994 and it has also linked more than 100 institutes. ChinaGBN is a state public economic information network under the control of the former Ministry of Electronics Industry. It is still weak and competes only against ChinaNET in limited areas. The networks currently can access one another only at very slow speeds. Access to ChinaNET from CERNET is possible only through an 8 Mb/s bandwidth. The integration of the nets will increase speed to 155 Mb/s it is believed.[10]

Use of the Internet has also spawned a growth industry of Internet police. The authorized size of this unit is more than 300,000 personnel. The police are designed to fight the flow of "harmful information" nationwide, to fight viruses and Internet crime. Organized into public information network supervision departments, the goal is to manage the Internet in accordance with the law, strengthen supervision, focus on prevention, ensure the stability of key points, and promote development while guaranteeing safety. College students have been recruited to help where possible.[11] Police control of the Internet, or at a minimum its monitoring, appears to be vital for future success in the opinion of most Chinese leaders. On 19 June 2001, newspapers carried an account of a Chinese businessman who was sentenced to three years in prison for posting articles critical of Chinese leaders and the ruling Communist Party on the Internet. He was charged with incitement of subversion, according to a report from the *Xinjiang Daily*.[12] Earlier, on 7 January 2001, another control mechanism was under consideration. Several unidentified companies agreed to form the China C-Net Strategic Alliance, a second-generation Internet-like network for China's government and industry. No start dates for construction or completion were offered. The *Xinhua News Agency* release noted that "the current one [Internet] has too many faults and is incapable of satisfying the needs of the Chinese government and companies as they enter the digital age." It is unknown whether foreigners will have access to the net, or if it will be compatible with the existing net.[13]

In October and November of 2000, the Chinese government established laws governing ownership, content, and other aspects of Internet use. The October set of laws limits direct foreign investment in Chinese Internet companies, requires companies to register with the Ministry of Information Industry and apply for permission before issuing stock or signing any agreement with a foreign investor, and bans the dissemination of any information that might harm unification of the country, subvert the government, or endanger national security. All Internet service providers (ISPs) must monitor content and restrict controversial topics in their chat rooms. Thus, the providers turn into *de facto* spies for the government.[14] In November, regulations emphasized that special licenses must be obtained by sites desiring to publish news. These sites may not generate their own news content, and can publish only stories from official sources.[15]

Shanthi Kalathil has provided the most interesting report on state controls over the Internet in China. Controls are necessary since China's educated professionals now have access to the Internet and are becoming more and more aware of the disparities between China and the rest of the world. Private sector development can also challenge state control in the economy and political spheres. Finally, the Internet offers dissidents and activists an unexpected outlet for their platforms. Kalathil listed both reactive and proactive responses. For reactive measures, she cited the desire of

Chinese authorities to filter material and promote self-censorship. The latter includes "encouraging" Internet café owners to keep a close eye on web surfers. For proactive measures, she noted that the government is becoming "informationized" since an e-government plan was devised. Further the government has learned how to distribute on-line propaganda and encourage what Kalathil calls "thought work." China is also considering the creation of a Chinese Intranet, is developing an information warfare strategy, and is using web access as a means of gaining popular support and legitimacy from the population.[16]

2. China's Information Technology Sector

The Ministry of Information Industry (MII) formulates national strategies and policy and plans for China. It also oversees special military networks and supervises telecom and information service markets. A military electronics industry bureau is part of the Ministry's internal setup. MII was created in 1998 by combining the Ministry of Post and Telecommunications and the Ministry of Electronics and Information. As a super-agency, it oversees telecommunications, multimedia, broadcasting, satellites, and the Internet.

A survey of China's information technology industry was completed in June 2000. It was divided into four parts: (1) telecom products and services, which were subdivided into four parts in 1999, China Telecom, China Mobile, China Satellite, and China Unicom; (2) computer products and services; (3) information appliances; and (4) audio-video entertainment. This and similar surveys will serve as the "investment guide" for the industry according to the report.[17] Simultaneously, China has increased its share of the domestic market for geographical and mapping software. Five years ago, domestic software companies held almost no portion of the Chinese market for these products, but today that share has increased to 28.9 %.[18] In February of 2001, Culturecom Group announced it would develop alternate versions of Chinese 2000 (Linux) to meet the needs of specific linguistic and cultural groups among the Chinese-speaking population.[19] Beijing has reported that the municipal government has approved 221 new software companies in 2000, positioning it to soon become China's largest software production center.[20]

China's State Council has invited investment in the software and integrated circuit industries. The 10th Five-Year Plan (2001-2005) plans on earmarking funds for the software and integrated circuit industries, as well as tax breaks for software enterprises. The integrated circuit industry will also receive preferential treatment, although not to the extent that the software industry will enjoy.[21] The 10th Five-Year Plan also envisages the infusion of $ 500 billion into the information technology sector. Development strategy is focused on e-commerce, broadband infrastructure construction and information development. Liu He, vice director of the State

Information Center, added that relevant laws and regulations should be improved, as well as the transparency of market rules. Protection of intellectual property and increased investment in human resources should be expanded too.[22] The information technology industry surpassed the power industry for the first time and is now the most profitable industry in China; and China's Minister of Information Industry Wu Jichuan predicted that China's information sector would grow by 20 % in the next five years.[23] The world's largest information technology center recently opened in Guangdong province on 19 December 2000 in Dongguan. The new center is both traditional and virtual, with clients able to view products, place orders and make payments online.[24]

One of the people most responsible for breaking up telecom monopolies, opening the Internet to China's massive middle class, and steering hundreds of millions of dollars of state money to venture investments is a rather unlikely source. He is Jiang Mianheng, son of President Jiang Zemin, and he is helping to modernize China from behind the scenes, outlining strategy and securing funding. His flagship company is China Netcom, which is building a 5,300 mile fiber-optic network linking 50 million people in 17 of China's most prosperous cities. China Netcom was originally created to build a broadband IP network. Rupert Murdoch and Michael Dell have invested $ 325 million in China Netcom. Jiang got his doctorate in high-temperature superconductivity from Drexel University in Philadelphia in 1991, and then worked for Hewlett-Packard for 18 months.[25]

Jiang hopes to set up a communications network to turn China into one of the countries with the highest density of Internet users in the world. In November of 2000, Jiang broke ground with Winston Wang, son of Taiwan private industrial chairman Wang Yung-ching, after coming to an agreement on a $ 1.63 billion computer-chip plant. There has never before been an economic bond of this magnitude that could eventually become the bridge for a political settlement between Beijing and Taipei. China already has six semiconductor foundries that make circuit-etched silicon wafers. NEC of Japan built one plant in Shanghai two years ago, and Motorola is building a plant in Tianjin. The Jiang-Wang plant is the first of four that the two plan to build on a 60-acre plot Shanghai.[26]

3. The Military and the Internet

The growth of the Internet in China also included the military sector. Reports out of China indicated in August 2000 that there were more than 400 military websites. Some support the PLA directly, such as the PLA internal information network. This "Intranet" has found a place in the political room of many units. Now, instead of reading Marxist-Leninist tracts soldiers can look up foreign military equipment on the web and read other interesting military-related information. Former PLA officers are

establishing some sites [27] and the PLA reserve forces have web sites too (i.e., http://ezarmy.net, the web site of the Echeng Reserve IW unit). *Jiefengjun Bao* established an Internet version of the PLA General Political Department's newspaper (www.pladaily.com) on 1 October 1999. The site discussed topics as varied as the 50th anniversary of National Day, the return of Macao, China's successful launch of the Shenzshou spacecraft, sessions of the National People's Congress, the development of the Western region of China, the study of the "three represents," the Taiwan issue, and criticism of the Falungong. This made one PLA officer stationed abroad proclaim, "we are very close to Beijing all of a sudden."[28] The paper also maintains links with journals such as the *Chinese National Defense Journal*, *Militia of China, Journalism* and *Self-Cultivation*, and *PLA Pictorial*.[29] WebPages on the Internet Version include Military Observation, Military Science and Technology, Joint Logistics for the Three Armed Services, Political Work, Weaponry, Windows on Foreign Armies, Military Pictures, Chinese Military Academies, Armed Police of China, Militia of China, Military Projects for National Defense, Military Circles History, Noted Military Surgeons, and Military Bookstore, among others.

For a period of time the number one site was Knowledge about Vessels (KAV) but the site soon merged with China's number one civilian site, Sina.com. After the KAV-Sina union, Chinese Youth Online began a military site named Chinese Youth Beacon on 1 August 2000. KAV has six "mottled bamboos" in its military forum. They are designed to check up on web users to ensure that secrets are not being passed around without notice. Another very popular web site is PLA pictures (www.plapic.com.cn), which has a huge variety of photos of military exercises, current events involving the PLA and President Jiang, photos of Chinese landscapes, and sixteen Internet connections. Some of the sixteen sites include:

- www.pladaily.com
- www.peopledaily.com
- www.sina.com.cn
- www.china.net
- www.xinhua.org
- www.globalizationforum.org
- www.top81.com.cn, and
- www.999junshi.com.

The site is updated with new pictures and with new current events on a frequent basis.

The military has become a popular topic lately, especially in light of Chinese reactions to the continuing tension with Taiwan, the war in Kosovo, and the recent incident involving the US reconnaissance and surveillance aircraft. Some non-

military web sites have added military pages, such as Xinhua Net's Junshi Tiandi (Military Sphere), Zhongxin Net's Junshi Tiandi (Military Sphere), Zhong Qing Zaixian's Zhong Qing Genghuo (China Youth Beacon, at www.cyol.net), and the military section of Xinlang Net (New Wave Net).[30]

There are several additional reasons for this popularity. First, the military sphere is changing quickly. There are new local wars and conflicts, and new generations of weapons. Due to the net, military news is not as opaque or semi-transparent as it once was. Second, the people are simply more interested in military affairs now that China has stepped into the center of world attention. On occasion it has happened that the more military information a site publishes the more hits it receives. Third, many military enthusiasts in China have never had an opportunity to publish about military affairs before the advent of the net. This offers many such individuals a chance to air their own point of view. Finally, several military news media and scientific research and teaching units are using the net. This includes *Jiefengjun Bao* (Liberation Army Daily), and the *Jiefang Huabao* (PLA Pictorial) of the Academy of Military Sciences.[31]

Fan Tao of the Military Law Department of the Xi'an Academy of Political Science believes that people's increased concern over national defense, and the diversification that the web offers to military education are other reasons for the web's popularity. Increased interaction among young web participants, that free one from time and space restrictions, increase its influence as well. However, not all web sites are as responsible and regulated as they should be. Some publish false information and irresponsible political views. Author Wei Daqing, writing in the newspaper *Zhongguo Guofang Bao* (sponsored by the PLA Daily three times a week), recommended increased control by network monitoring and management departments, and information security departments.[32] On 10 February 2001 *Jiefangjun Bao* noted that the Central Military Commission went a step further. It issued Provisions to the four general departments of the PLA on the Security and Confidentiality of Computer and Information Systems. The Provisions were designed to boost Internet security as well as military computer security.[33] On 2 May this warning was repeated in *Jiefangjun Bao*. Reporter Li Min stated that comrades of "network management" departments must conduct thorough investigations, issue warnings in a timely manner and expel from the Internet those who refuse to correct mistakes after repeated disciplinary action.[34]

Finally, the Internet has provided the means for PLA war games on occasion. For example, in July of 2000, the Chengdu Military Region conducted a confrontational campaign exercise on the Internet. The three training tasks associated with the exercise included organizing and planning the campaign, striving for air and

information control, and making and countering breakthroughs. Over 100 terminals were linked for the exercise.[35]

4. Two 1999 Internet Wars: China vs. NATO and China vs. Taiwan

In May 1999 a US guided missile slammed into the side of the Chinese Embassy in downtown Belgrade, Yugoslavia. The Chinese Liberation Army Daily (LAD) disclosed on 27 July 1999 that a "network battle" was fought between Chinese and US hackers following the 8 May bombing of the Chinese embassy. US hackers, according to the report, aimed their counterattack at the following web sites: Xin Lang Wang or Sina (http://home.sina.com.cn), Zhongwen Re Xun or Yesite (http://www.yesite.com), and Shanghai Wang Sheng or Shanghai Web Boom (no URL listed). The Chinese initiated the US hack by altering the home page of the US Embassy in Beijing, writing on it "down with the Barbarians."[36] The Chinese also report causing a blackout at a few US political and military web sites, and some 300 civilian web sites. In all Chinese hackers broke into nearly 1,000 US civilian web sites and coordinated an attack on NATO computers.[37]

The methodology for performing these hacks, according to the LAD article, was the mobilization of thousands of net users to issue a ping command to certain web sites at the same time. This caused servers to be overloaded, and paralyzed these websites. In addition, thousands and thousands of e-mails were sent daily to the opposite side, thus blocking mail servers. Viruses were sent via e-mail, and attacks were launched with "hacker tools" hidden in certain programs. The LAD article called for developing a computer network warfare capability, training a large number of network fighters in PLA academies, strengthening network defenses in China, and absorbing a number of civilian computer masters to take part in actions of a future network war.[38]

There was also an Internet war with Taiwan. In June Of 1999, Taiwanese President Lee Teng-hui stated that PRC and ROC ties should be based on special state-to-state relations. This infuriated the PRC, with Beijing calling Lee a "demented test-tube baby." Nearly two months later, on 8 August, a cyber war started between the two. Taiwan blamed China for starting it, and China blamed Taiwan. Taiwan's hackers reportedly attacked the PRC's State Tax Authority website and the Ministry of Railways site. One hacker threat was that on 1 October, China's National Day, all Chinese web sites with simplified Chinese characters would be hit with viruses. Chinese hackers, for their part, broke into Taiwan's Inspector General web site, and the web sites of the Investigation Bureau of Taiwan's Justice Ministry, the Ministry of Economic Affairs, the National Assembly, and the American Institute in Taipei, the unofficial embassy of the US in Taiwan.[39] The MSNBC website estimated that, in all, Chinese compatriots launched more than 100,000 attacks on Taiwan government sites.

5. The Internet War with the US over the EP-3 Reconnaissance and Surveillance Aircraft

On 1 April 2001, a US EP-3 reconnaissance and surveillance plane approached China's Hainan Province via the South China Sea. Two Chinese F-8 jet fighters scrambled to meet it. Unfortunately, one of the planes, piloted by Wang Wei, collided with the US plane. The latter and its crew, due to damage done to the plane, was forced to land on Chinese territory at Lingshui Airport in Hainan. Initially, discussion about the incident was centered in chat rooms in China and the US. In China, citizens expressed their indignation and offered potential solutions to this situation in chat rooms throughout the country. Sina.com, Sohu.com and Chinadotcom Internet chat rooms were the most popular web sites in China. Chinadotcom conducted a survey to find out the feelings of citizens. Some 60,962 citizens reportedly participated. The survey indicated that 18 % felt China should remain unyielding, 15 % took the action as an act of war, 22 % said keep the plane for examination, 25 % said free the plane, and only 3 % recommended getting to the bottom of the incident with an investigation.[40] Some of the comments reported in the chat rooms included:

- "This is the third time the American imperialists have dumped crap down China's neck."
- "We can forego joining the WTO but we cannot afford to loose face."
- "We should calm down and find out the truth."[41]
- "Why can't the US show any human rights concern to the poor missing pilot?"
- "The whole nation is waiting to see if China can play hardball with the US."[42]

Two hacker groups took center stage in the US, Pr0phet and Poizonb0x. On 11 April, the first Pr0phet political reference was made, and on 14 April the first Poizonb0x defacement of a Chinese site occurred. One attack site read "bagel-morning coffee- and a Chinese website. Nice little routine." Concern was great, and the National Infrastructure Protection Commission's Watch and Warning Unit gave out its phone number (202-323-3204/05/06) and a web site (NIPC.Watch@fbi.gov). Hotlines were established at http://www.fbi.gov/contact/fo/fo.htm and http://www.NIPC.gov/incident/cirr.htm. A list of many of the hacks is available at http://attrition.org/mirror/attrition.[43]

In China, there were three groups responsible for most of the defaced web sites. They included Honker Union of China, Hacker Union of China, and China Eagle Union, a civilian nonprofit organization of part-time network enthusiasts. Provincial groups organized some Chinese attacks. They included the provinces of Fujian, Hubei, and

Guangdong among others. Perhaps these groups included the PLA reserve groups of IW battalions, but this was never made clear. The Chinese used several hacker tools such as killUS and DNSKiller. The State Computer and Network Emergency Handling and Coordination Center, China Computer Network Emergency Center (www.cert.org.cn) handled the Chinese web problems.[44]

Soon, Netor.com, a leading host of mourning sites in China, established an online shrine to Wang Wei. Here citizens could light a virtual candle, leave digital flowers, dedicate digital melodies ranging from traditional Chinese music to the theme songs from Titanic or Ghost, or offer written expressions of their grief online. "We salute the hero in the sky," wrote one, while another citizen said, "You have fallen but millions like you live on to fight for the motherland." In just three days Wang's site received the third most visits of any of the nearly 5,000 hosted by Netor.com.[45]

Slowly, the defacing increased and a hacker war was declared for the dates of 30 April to 8 May. Pamela Hess reported on 30 April in Infospace.com that spokesman Lt. Cdr Reif stated that the Navy was at INFOCONALPHA, a cyber version of the physical threat condition. The Navy's Fleet Information Warfare Center announced its status on 26 April, and the JTF CND on 30 April. So both governments were taking this small cyberwar between individuals very seriously.

Individuals from many nations participated, with Saudi Arabia, Pakistan, India, Brazil, Argentina, and Malaysia on the US side and Korea, Indonesia, and Japanese hackers supporting China. Some, such as Brazil, supported both. It was clear that a cyber mob mentality had developed. Chinese hacker Jia En Zhu, who lives in a Beijing suburb, wrote, "Many people here are frustrated with America." China's attack was planned for 1-7 May, peaking on 4 May, a Chinese holiday commemorating the country's first major student demonstration that took place, ironically, in Tiananmen Square 82 years ago.[46]

A Chinese National Defense University Professor dubbed this cyber war "extremely important" on 11 May. Professor Zhang Zhaozhong, a renowned military expert and director of the Military and Equipment Teaching and Research Center, stated that the cyberwar

> "… presented a modern format of warfare, alive and kicking, before the eyes of the netizens, and invented many a combat method through practice, amassed abundant experience, expanded the contingent of hackers, tempered their mettle for cyberspace fighting, and made an impressive show of the wisdom and abilities of the Chinese netizens to the netizens around the world. … This cyberwar was by nature a counteroffensive for self-defense and was an act of defensive counterattack compelled by the strong offensive from hackers of the opposite side."[47]

6. Conclusions

This overview of the civilian and military aspects of the Internet in China reveals several interesting issues. First, of course, is the rapid growth of Internet users in both sectors. If *Red Herring* is correct, the figure of 130 million Internet users by the year 2005 is simply astounding for a nation often accused of being too backward to present any type of threat in the immediate future. China also appears capable, with the work of Jiang Zemin's son and others, of putting together a formidable computer industry that will be home grown. The sheer number of Chinese software writers and mathematicians should ensure a healthy future for the Chinese computer industry.

Second, the idea of 130 million potential Internet users coupled with the idea that the Internet might be used by the military, as Shen suggests, as a means to implement 36 ways to disrupt the Internet is worthy of much closer inspection. Perhaps the reserve IW forces of the PLA that are currently used by the military as an opposing force in military exercises will bear the brunt of the mission to perform the disruptions. It is doubtful if foreign military observers will be able to distinguish between civilian hackers and reserve force hackers in a future Internet confrontation. It should be remembered that the IW reserve force in Xian has already become somewhat infamous for its development of 10 methods to attack computers. These ten methods are: planting information mines; conducting information reconnaissance; changing network data; releasing information bombs; dumping information garbage; disseminating propaganda; applying information deception; releasing clone information; organizing information defense; and establishing network spy stations.[48]

Third, the military has found several uses for the Internet other than providing an OPFOR mechanism for reserve forces. The Intranet in political rooms offers young soldiers a chance to use computers, and to actually access PLA databases of foreign military equipment. In one instance, the Internet served as the mechanism for an entire IW exercise in the Chengdu military region. Important academies and institutes in China maintain several other military sites.

Finally, the Internet battles that have erupted between China and NATO, Taiwan, and the US are worthy of our immediate concern. They demonstrated the ability of citizens (or military members cloaked under the guise of civilians) to conduct cyber attacks on one another's systems, and to increase tensions between two sides. This is a dangerous precedent in a world sadly lacking in regulation in this area, if indeed regulation is even possible. The involvement of the FBI and the raising of the threat status among US Navy personnel to INFOCONALPHA, a cyber version of the physical threat condition, are indicative of the growing seriousness of this issue.

What does the future hold? Clearly it appears that the future will offer even more problematic scenarios for military forces around the world. The inability to determine

who initiated an Internet attack and what is the intent of the electrons involved in the attack will continue to haunt intelligence and operational staffs in the coming months and years. The Internet may indeed play a bigger role in our military future than any of us originally believed.

DISCLAIMER: The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the US government. The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open source media and direct engagement with foreign military and security specialists to advise army leadership on issues of policy and planning critical to the US Army and the wider military community.

Notes:

1 Shen Weiguang, *The Third World War—Total Information War* (Xinhua Publishing House, January 2000), as translated and downloaded from the FBIS web site on May 17, 2000, http://199.221.15.211/.

2 Ibid.

3 "Greater China online population hits 24 million," *Taipai DPA* (January 23, 2001).

4 "China Internet Users grow to 22.5 million," *Muzi.com Website* (January 17, 2001), http://www.muzi.com/.

5 "Portal Personification: Survey Tracks Netizens' Use, Opinion of Net," *Inside China Today* (May 3, 2001), http://www.europeaninternet.com/china/.

6 Ibid.

7 "Asia at a Glance," *Red Herring* (October 2000), 115. Available @ http://www.redherring.com/.

8 Nina Hachigian, "China's Cyber-Strategy," *Foreign Affairs* (March/April 2001), 119, 120.

9 "69 million mobile Internet users in China by 2000," *Muzi.com Website* (November 16, 2000).

10 "China to Link Four Backbone Internet Networks," *ChinaOnline Website* (March 23, 2000). Available @ http://www.chinaonline.com/.

11 "Internet police ranks swell to 300,000," *'Ming Pao' web site* (Hong Kong, December 8, 2000), www.mingpao.com/newspaper/.

12 "China Sentences Critic," *The Kansas City Star* (June 19, 2001), A8.

13 Beijing, *The Associated Press* (January 8, 2001).

14 "Cracks in the Great Firewall," *World Press Review* (May 2001), 11, 12.

15 Hachigian, "China's Cyber-Strategy," 124.

16 Shanthi Kalathil and Taylor C. Boas, "The Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution," *Carnegie Endowment Working Papers*, Global Policy Program, Number 21 (July 2001), 6-10.

17 "China completes nationwide IT survey," *ChinaOnline Website* (June 5, 2000).

18 "China puts itself on the software map," *ChinaOnline Website* (August 16, 2000).

19 "Survival of the Linux: Software adapted to meet different cultural needs," *ChinaOnline Website* (February 28, 2001).

20 "Bejing moves to upgrade software industry," *ChinaOnline Website* (March 20, 2001).

21 "State Council encourages development of software, integrated circuit industries," *ChinaOnline Website* (July 14, 2000).

22 "U.S. $500 billion slated for IT sector by '05," *ChinaOnline Website* (April 23, 2001).

23 "China Targets 20% Annual Growth for Information sector in Five Years," *Chinatopnews.com* (May 8, 2001), http://www.chinatopnews.com/.

24 "World's largest IT center opens in Guangdong," *ChinaOnline Website* (December 27, 2000).

25 Joanne Lee-Young, "The Digital Prince of China," *The Industry Standard* (2000).

26 Craig Smith, "A Chip Plant That is Full of Symbolism," *The New York Times* (November 24, 2000), from the New York Times web site on 24 November 2000.

27 Wei Daqing, "On the Sudden Emergence of Military Websites," *Zhongguo Guofang Bao* (November 6, 2000), 4, as translated and downloaded from the FBIS web page on 14 December 2000.

28 Li Guohua, "Open Up New Field for Dissemination of Military News," *Jiefangjun Bao* (October 4, 2000), 2, as translated and downloaded from the FBIS web page on 4 October 2000.

29 Ibid.

30 Ibid.

31 Ibid.

32 Wei Daqing, "On the Positive and Negative Aspects of Military Websites," *Zhongguo Guofang Bao* (November 6, 2000), 4, as translated and downloaded from the FBIS web site on 14 December 2000.

33 "Managing Internet According to Law is a Must," *Jiefangjun Bao* (February 10, 2001), 1, as translated and downloaded from the FBIS web site on 12 February 2001.

34 Li Min, "Network Mangers should Exercise Strict Management," *Jiefangjun Bao* (May 2, 2001), 1, as translated and downloaded from the FBIS web site on 2 May 2001.

35 Xu Wenliang and Wan Yuan, "Chengdu Military Region Conducts Long-Range Confrontational Exercises on Internet," *Beijing Jiefangjun Bao*, Internet version (July 10, 2000), as translated and downloaded from the FBIS web site on 10 July 2000.

36 "Military Forum" page, *The Liberation Army Daily* (27 July 1999), report obtained via e-mail from Mr. William Belk (June 1, 2000).

37 "Collision could Launch Wave of Hackers," *thedailycamera.com* (April 4, 2001).

38 William Belk's e-mail (June 1, 2000).

[39] Damon Bristow, "Cyber-warfare rages across Taiwan Strait," *Jane's Intelligence Review* (February 2000), 40.

[40] Rachel Morarjee, "AFP: PRC Web surfers call for PRC to 'Play Hardball' with U.S. on Air Collision" (Hong Kong, April 4, 2001), as translated and downloaded from the FBIS web site on 4 April 2001.

[41] "AFP: Chinese Websites Protest U.S. Plane Incursion" (Hong Kong, 2 April 2001), as translated and downloaded from the FBIS web site on 2 April 2001.

[42] Rachel Morarjee, "AFP: PRC Web surfers call for PRC to 'Play Hardball' with U.S. on Air Collision."

[43] Carl O. Schuster and Anthony Miccarelli, "Special Press Summary: China's May Day Cyber War," a product of the Virtual Information Center (no date).

[44] Ibid.

[45] Clay Chandler, "For Chinese Pilot, Martyrdom on Earth and in Cyberspace," *The Washington Post* (18 April 2001).

[46] Michelle Delio, "Technology: U.S., Chinese hackers vow to wage online war," *Agence France-Presse* (April 21, 2001).

[47] Interview with Zhang Zhaozhong, "Military Expert Comments on 'May Day' Cyber War between China and the United States," *Guangzhou Ribao* (May 11, 2001), as translated and downloaded from the FBIS web site on 12 May 2001.

[48] *Qianjin Bao* (December 10, 1999), provided by Mr. Belk via e-mail.

Timothy L. Thomas is an analyst at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. He retired from the US Army as a Lieutenant Colonel in the summer of 1993. Mr. Thomas received a B.S. from West Point and an M.A. from the University of Southern California. He was a US Army Foreign Area Officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute (USARI) in Garmisch, Germany; as an inspector of Soviet tactical operations under CSCE; and as a Brigade S-2 and company commander in the 82nd Abn Division. Mr. Thomas has done extensive research and publishing in the areas of peacekeeping, information war, and political-military affairs. He is the assistant editor of the journal *European Security*; an adjunct professor at the US Army's Eurasian Institute; an adjunct lecturer at the USAF Special Operations School; and a member of two Russian organizations: the Academy of International Information and the Academy of Natural Sciences. You may forward comments referencing this study to: FMSO, ATZL-CTL, Mr. Thomas. 101 Meade Avenue, Ft Leavenworth Kansas 66027-2322. *E-mail*: ThomasT@Leavenworth.army.mil