CSA2011809

CHINASCOPE Analysis Series

China's Cyberwarfare

November 2011

Summary: China is spearheading a war in cyberspace. Reports about China's cyber-espionage or its attacks are mushrooming. A study of the available online information published in the Chinese media as well as the Western media leads to the conclusion that China has elevated cyberwarfare to a paramount strategic position and is fighting it using the "People's War" (人民战争) Approach.

China's Cyberwarfare

China is spearheading a war in cyberspace. Reports about China's cyber-espionage or its attacks are mushrooming. A study of the available online information published in the Chinese media as well as the Western media leads to the conclusion that China has elevated cyberwarfare to a paramount strategic position and is fighting it using the "People's War" (人民战争) Approach.

I. The Strategic Importance of the Cyberwar

The People's Liberation Army (PLA) considers the cyberwar to be highly significant and places it in high regard. Some PLA experts have elevated its importance to the same level as or even above a nuclear war.

1) The Definition of Cyberwar

One *PLA Daily* article posited the following definition: "A cyberwar is the offensive and defensive actions taken to interrupt and destroy the enemy's network system and to protect the safe operations of ones own network system. It is a fight in cyberspace in which two rivals apply cyber-technologies in political, economic, military, and technological fields to gain an information advantage." [1]

Several military articles have suggested that a cyberwar has a wider meaning as well as a narrower one. One article in *PLA Daily Online* suggested, "The wide definition of a cyberwar is that two rivals engage in a fight in the political, economic, military, and technological fields by applying cyber-technology to obtain an information advantage. The narrow definition is that the rivals conduct a series of cyber-surveillance, cyber-attack, cyber-defense, and cyber-support actions in the area of battle command, weaponry control, battle support, logistics and supply, military training, surveillance, and battle management." [2]

Even from the narrower point of view, the PLA understands that cyberwarfare goes far beyond hacking websites. One PLA expert outlined a few examples of cyberwar actions. These include attacking the U.S. Department of Defense's (DOD's) websites, entering the Pentagon's database to steal the secrets for controlling nuclear weapons, issuing orders to U.S. troops by pretending to be U.S. military commanders, destroying U.S. data connections, and blocking the U.S. military communication channels between land and space or between different military units. [3]

More importantly, in the PLA's mind, a cyberwar is much more than a military action. Li Daguang, China's cyberwar expert and a professor at the Defense University argued, "I believe that future information warfare will be fought on two levels. One is the 'hard' battle of traditional warfare, which is the fire and blood in 'five dimensions,' that is, land, sea, sky, space, and electronics. Another is the 'soft' battle in cyberspace, involving culture, technology, physiology, the economy, and finance. This 'soft' battle is being fought every day." [4]

Clearly, the Chinese military experts view cyberwars as comprehensive, occurring in the political, economic, technological, social, and cultural realms.

2) The Strategic Importance of Cyberwars in the Military's Eyes

China has long recognized the important of cybersecurity and cyberwarfare. At the Fourth Plenary Session of the Sixteenth Central Committee of the Chinese Communist Party (CCP) in 2004, China listed "information security" as a critical issue impacting national security. [5]

In the PLA's eyes, cyberwarfare is the most significant warfare in the information era. This can be seen by the many Chinese military publications, which repeatedly quote a RAND Corporation study saying that strategic warfare in the industrial era was nuclear war, while in the information era it is cyberwar. [6][7]

Li Daguang painted a frightening picture of cyberwarfare, "When the network is paralyzed, we will lose control of our satellites, financial transactions will cease, and there will be no electricity. Even factories and chemical plants may explode. … Some even say, 'A cyber attack is comparable to a nuclear attack.'" [8]

One PLA article stated that "the threat of a cyberwar is greater than that of a nuclear weapon" as it can be very destructive. "People tend to think that a cyberwar is more civilized than traditional warfare and that it can achieve its war objectives with less blood or even no blood. Actually, that's not the case at all! Experts predict that a cyberwar will paralyze the earth in an instant!" "When a cyberwar starts, the country being attacked faces the danger of the complete collapse of its entire economy."

The article went further to argue that the real power of a cyberwar is the psychological impact. "From the viewpoint of strategic position, a cyberwar is as important as a nuclear weapon. To a certain extent, it may be even more significant than a nuclear weapon. For example, a nuclear weapon can create huge psychological distress. A cyberwar also does great damage to people mentally. Attacking people's minds and spirits can extinguish their will to fight and sense of determination. Currently, studies

on cyberwarfare tend to focus on techniques, but the real power of a cyberwar is to attack the enemy mentally and spiritually." [9]

3) War Defined in *Unrestricted Warfare*

The book *Unrestricted Warfare* (超限战) described a new type of warfare with "irresponsible and destructive characteristics which disregard rules" as follows:

"The direct result of the destruction of rules is that the domains delineated by visible or invisible boundaries which are acknowledged by the international community lose effectiveness. This is because all principals without national power who employ non-military warfare actions to declare war against the international community all use means that go beyond nations, regions and measures. Visible national boundaries, invisible internet space, international law, national law, behavioral norms, and ethical principles, have absolutely no restraining effects on them. They are not responsible to anyone, nor limited by any rules, and there is no disgrace when it comes to the selection of targets, nor are there any means which are not used. Owing to the surreptitious nature of their movements, they have very strong concealment, create widespread damage because of their extreme behavior, and appear unusually cruel as a result of their indiscriminate attacks on civilians. All of this is also broadcast through real time via continuous coverage by the modern media which very much strengthens the effects of terrorism. When carrying out war with these people, there is no declaration of war, no fixed battlefield, no face-to-face fighting and killing, and in the majority of situations, there will be no gunpowder smoke, gun fire, and spilling of blood. However, the destruction and injuries encountered by the international community are in no way less than those of a military war." [10]

The description of this type of war applies almost perfectly to a cyberwar.

4) Why China Pays So Much Attention to Cyberwar

Why does the PLA show such great interest in and fondness for cyberwarfare? It is because a cyberwar presents not only a significant destructive force in the physical, political, economic, and psychological world, it also gives the PLA a shortcut opportunity to close the gap with the U.S. militarily. Compared to conventional warfare, cyberwarfare does not require an extensive capital investment. "The cost to carry out a 'computer cyberwar' is much less. In essence, the strategies implemented by a nation's cyber army would be no more than the attack and defense tactics used by elite hackers in a well-equipped and well-conditioned Internet cafe. The entry fee for carrying out these tactics is so minimal that even someone without professional

training can do it." [11] This makes it possible for the PLA to close its information technology gap with the U.S. much faster than if it were to try to compete with traditional weaponry.

Furthermore, China has a given advantage over the U.S. in cyberwarfare: people. China has an abundance of talent either to serve directly or to supplement its cyber army. China has been cashing in on this advantage and adopting a "People's War" approach to build up its cyberwar "arms" chest.

II. Using the "People's War" Strategy (人民战争) to Win a Cyberwar

Wikipedia has defined the "People's War" strategy as a military-political strategy invented by Mao Zedong. The basic concept behind a People's War is to maintain the support of the population and draw the enemy deep into the interior, where the population will bleed them dry through a combination of mobile warfare and guerrilla warfare. [12]

The PLA was extremely successful in applying the "People's War" strategy against the Kuomintang, or the Chinese Nationalist Party, from 1946 to 1949. The PLA mobilized people in the area that they controlled to support them. People gave their support in multiple ways: by joining the army, by joining the militia to fight guerrilla wars to support the army, by providing combat-related labor (such as carrying food and military supplies to the front lines), by donating food and supplies, and so on. A propaganda campaign played a major role in getting people to support the war voluntarily. The strategy worked very well. In 1949, the CCP took over China's entire mainland, even though, at the beginning of the war in 1946, it had actual control over less than a quarter of the total land area and about a quarter of the population.

The "People's War" provides the PLA with a huge supply of warm bodies. This enables the PLA to adopt the "human-wave tactic" (人海战术) in combat. The U.S. army saw this carried out many times in the Korean War when fighting against the PLA, which entered the war under the name "Chinese People's Volunteer Army." This military strategy makes use of, and sacrifices, a large number of people in combat to make up for technical and military disadvantages.

Applying the "people's war" strategy and the "human-wave tactic" to cyberwarfare enables a combatant to: conduct a propaganda campaign; mobilize the people; build up a huge cyber-attack resource base that includes military staff, hackers, private companies, and Chinese netizens; use both the military and private companies to

develop cyberwarfare technologies; and carry out the attack on multiple fronts (such as hacking, espionage, and other actions).

Wan Dongsheng, PhD, a cyberwar expert at the PLA's Electronic Engineering Institute, pointed out in his thesis in 2006, "Any confrontation between China and the U.S. in cyberspace is similar to the early wars that the PLA fought (against the Kuomintang)." Wan further explained, "It is less-developed technology against advanced technology and a large number of people against a smaller number of people. China might lose a lot of ground in the early stages of the war, but its guerrilla tactics can damage the enemy and make it pay a huge price." [13]

1) A Propaganda Campaign to Build Public Support

To build public support, Chinese media have created a sense of crisis about cyberwars and reported how other countries were developing their cyber armies.

Deputy Direction Zhang Li of the Security and Strategy Institute at China's Institute of Contemporary International Relations described other countries' preparation for cyberwar as "sharpening the knife to get ready and pressing harder and harder (against China)." [14]

A *PLA Daily Online* article reported, "In January (of 2009), the U.S. DOD published its 2009 Quadrennial Roles and Missions Review, listing 'cyberspace war' as one of the U.S.' Core Mission Areas.

"Shortly thereafter, President Obama ordered a 60-day review of the U.S. national cybersecurity status and announced the position of 'cyberspace czar' to manage national cybersecurity affairs and prepare for future cyberwars.

"On May 29 (2009), the U.S. Strategic Command announced that they were recruiting 2000-4000 soldiers to form a 'special unit' for cyberwar.

"On June 23 (2009), the U.S. Defense Secretary formally announced the establishment of a cyber command to consolidate U.S. cyberwar capability.

"Other countries also smelled danger from cyberspace. They started recruiting cyberwar soldiers, to protect own countries' cyber security.

"South Korea plans to establish a cyberwar command and openly recruit soldiers with career specialists skilled in information defense. …

"India is building a 15,000-person cyber security team. …

"Germany plans to build a 6,000 person cyberwar army to respond to the emergencies occurring in cyberspace. It has been said that this troop has already been conducting cyberspace monitoring in Afghanistan." [15]

A *Xinhua* article stated, "The U.S. now has the world largest 'cyberwar' army. Besides the U.S., other countries, including the United Kingdom, Japan, Russia, Israel, India, and South Korea, also take the possibility of a 'cyberwar' very seriously. News is frequently published about their recruiting hackers and setting up a special cyberspace attack and defense army." [16]

This alarming technique apparently is working. After U.S. Secretary of Defense Gates announced on June 24, 2009, that a Cyber Command would be established, *Huanqiu,* a media under *People's Daily*, hosted an online survey asking, "Do You Think China Should Set up a Cyber Command?" By 8 a.m. on June 28, over 4,000 people had cast their votes. Ninety-four percent (3823) voted Yes. [17]

2) Mobilizing the Population

Wan Dongsheng argued that "the public needs to be mobilized to fight a lasting guerrilla war over cyberspace. The military and government should work together to plan an integrated cyberwar. They need to offer professional direction, train, and organize the several hundred million netizens in China." [18]

PLA Daily Online offered a detailed account of how the Shaoyang Military Sub-region and the Shaoyang Municipal National Defense Mobilization Committee in Hunan Province educated the public:

"On April 18, when Yang Wenhuan, Director of the Computer Lab of the Shaoyang Municipal Statistics Bureau, paid his monthly Internet fees at an agent's desk set up in a bank, he received the quarterly national defense education packet. When he went back to his office and turned on his computer, he received an email – "Be a Patriotic Warrior in the Future Information War." Citizens in Shaoyang frequently received these educational packets and electronic mailings. They were not even aware that they were getting an education in national defense.

"The Shaoyang government established an Online National Defense Education Team, above the Multi-Media Communication Bureau. Led by the Multi-Media Communication Bureau and supported by colleges, key middle schools, and research institutes, the government surveyed the city's potential for cyberwar mobilization

(how many people can be mobilized to join the cyberwar). They educated netizens in national defense through multiple channels, including distributing education packets, sending emails, adding informational war materials in computer classes and national defense education classes at the colleges and high schools, and creating an education environment on websites or at Internet cafes." [19]

3) The Cybermilitia

Both the Chinese information security practitioners and the U.S. think tankers recognize that China has a "human resource advantage" on the cyberwar front. [20] The PLA has fully leveraged its advantage by building a cybermilitia.

As early as the beginning of the 21st century, if not earlier, PLA experts started advocating the concept of a cybermilitia.

One *PLA Daily Online* article in 2001 suggested, "The people's armed forces should target future warfare's real need and follow the following principles and methods to build cybermilitia units:

"First, select the (cybermilitia) resources citywide but with a focus. The companies that conduct network business or have a computer network should be the primary focus in forming militia units. In cities, the primary targeted companies are telecommunication bureaus, mobile telecom companies, paging companies, as well as businesses in the fields of transportation, finance, and electricity, and colleges, all of which have their own networks. Other companies will supplement them. Second, form units that are the right size, based on the local situation. (Militia unites in) mid-sized cities can be formed as battalions or companies and (those in) counties or districts can be formed as companies or platoons. Groups should be formed based on local conditions. If there are many people, form a big unit; if otherwise, a small one. Third, be practical in creating the militia units. When selecting resources, pick primarily those in software development and network research areas and supplement them with people who have hardware support and operations experience. Favor those with college or higher levels of education and level II certification in the National Computer Rank Examination. As for equipment, insist primarily on using a standard local network system and supplement it with non-standard network equipment." [21]

Another *PLA Daily Online* article in 2001 discussed how "people are to support a cyberwar battlefront." "The population will target the enemy's computers and networks, use advanced information technology, and be active in all of cyberspace to support the military in carrying out an information attack or information defense."

"In the future war, the population can support a cyberwar front in many ways. Some examples include using a computer virus to carry out a virus war; making the enemy's life-supply network fail; creating an 'information flood' by dumping false or outdated information on the enemy to block or occupy their storage space and communication channels and prevent them from transporting and processing the information they need; infiltrating the enemy's network system and using it to direct the enemy's actions; and use the network to connect to people overseas and break the enemy's information blockade so that we can mobilize our own nation, unite with our friends around the world, and develop a psychological combat field inside the enemy's territory." [22]

Three officers from the Jiangsu provincial PLA command's mobilization department wrote a paper that was published in *National Defense*, the magazine of the Academy of Military Sciences. In the paper, they discussed the cybermilitia's tasks include "stealing, changing, and erasing data" on enemy networks and their intrusion with the goal of "deception, jamming, disruption, throttling, and paralysis." It pointed out, "(These militias) should preferably be set up in the telecom sector, in the electronics and Internet industries, and in institutions of scientific research." [23]

A Northrop Grumman report to the US-China Economic and Security Review Commission said, "The PLA is reaching out across a wide swath of Chinese in the civilian sector to meet the intensive personnel requirements necessary to support its burgeoning information warfare capabilities, incorporating people with specialized skills from commercial industry, academia, and possibly select elements of China's hacker community." [24]

Financial Times recently reported on an example of a cybermilitia unit. The Nanhao Group, based in Hengshui (near Beijing), makes online scoring systems, exam-mark scanners, and other education hardware and software. Since 2005, it has been home to a cybermilitia unit. The company's vice president "confirmed that the local PLA command led its cybermilitia unit and had 'regular exchanges' with it, training the PLA officers." [25]

4) Military-Civilian Joint Efforts / Indigenous Innovation

To win the cyberwar, the PLA not only needs cybermilitia support; it also needs help from civilian companies and organizations. These military-civilian collaborations occur in a number of ways:

<u>Civilian Companies or Universities Train Military Staff</u>

A General Communication Station in the PLA General Staff Department has established a partnership with China Telecom, Beijing Co. (Beijing Telecom). "Beijing Telecom is responsible for training the staff for the communication station. Beijing Telecom sent several engineers and technicians to conduct over ten training sessions on new technologies on program-controlled exchange, data communication, broadband communication, secure communication, and satellite communication. Divisions of Beijing Telecom, including the mobile division, long-distance division, Zhongnanhai division, phone line division, and city line third district division, established a buddy relationship with units within the General Communication Station. These divisions offered technical training to soldiers in lower units." [26]

Military-Civilian Joint Efforts to Develop Indigenous Technologies and Innovation

PLA security experts have long been pressing for the development of network security technology and products. The participants in a conference in Jinan City, Shandong Province, held in 2000 stressed the importance of such development and made the suggestion "to combine the indigenous development and adoption of foreign technologies together, combine military development and civilian companies' development together, and combine basic technology research and the protection of technological research together." [27]

This led to the development of the Kylin system, a Chinese-built secure operating system. China started its development in 2001; in 2007, it installed the system on government and military servers. China has also developed a secure microprocessor that "is known to be hardened against external access by a hacker or automated malicious software." [28]

The super computer Tianhe-1 is another example of China's indigenous innovation. Designed and developed by the National University of Defense Technology, a military university, it is able to perform 2570 trillion computations in a second. In November 2010, it was recognized as the world's fasted computer. [29] Though it later lost out to Fujitsu's K-computer in June 2011, this still showcased the muscle of China's abilities in computer technology.

Using Civilian Companies to Obtain Technologies from Foreign Companies

China uses its local market to attract Western companies who have advanced technologies. To conduct business in China, these companies are forced to share their technology with their Chinese partners. U.S. Naval War College Professor Andrew Erickson warned about the situation in which General Electric (GE) is to share its commercial jet engine design technology with China: "Joint ventures with jet engine

market leaders like General Electric (GE) have the potential to give the Chinese aerospace industry a 100 piece puzzle with 90 of the pieces already assembled. Enough is left out so that the exporting companies can comply with the letter of the export control laws, but in reality, a rising military power is potentially being given relatively low-cost recipes for building the jet engines needed to power key military power projection platforms, including tankers, AWACS, maritime patrol aircraft, transport aircraft, and potentially, subsonic bombers armed with standoff weapons systems." [30]

Chinese companies can also purchase Western companies to obtain the technical know-how. "Kenneth deGraffenreid, former deputy national counterintelligence director, said China's strategic-technology acquisition efforts are similar to those used by the Soviet Union during the Cold War. 'But unlike the Soviets, the Chinese use companies that appear on the surface not related to the government, but they are,' Mr. deGraffenreid said. 'All these Chinese companies are part of state ministries, MSS or [military intelligence], and have interlocking structures and personnel.'" [31]

Then there is the increasing cyber-espionage originating from China. On November 1, 2011, Symantec reported on a large scale, ongoing hacking campaign by Chinese malware snooping around the computer networks of "multiple Fortune 100 companies involved in research and development of chemical compounds and advanced materials, companies that develop advanced materials primarily for military vehicles, and companies involved in developing manufacturing infrastructure for the chemical and advanced materials industry." The report said some 19 total companies "in the defense sector" were targeted in the hacking campaign, which apparently was designed to sniff out "intellectual property such as design documents, formulas, and manufacturing processes." [32]

5) Chinese Hackers

The Chinese military has long viewed hackers as a critical component in its war chest. Zhang Zhaozhong, Director of the Military Science and Technology Education and Research Office at the National Defense University, suggested that "utilizing (the hackers) to the maximum extent and combining them with the legal and underground forces will rapidly improve our nation's information security level." [33]

<u>China's World-Class Hacker Army and Their Sense of Patriotism</u>

LION and the association that he created and leads, the Honker Union of China (HUC, 中国红客联盟) is the best known hacker name in China. According to the

encyclopedia of the search engine Baidu, the HUC was "formed in 2000 by the legendary hacker LION. At its peak, it had over 80,000 members and ranked fifth in the world. Its most famous action was the denial of service (DOS) or distributed denial of service (DDOS) attack on the White House in 2001." [34]

The "attack on the White House," as discussed on Baidu, is one of the wars between Chinese hackers and U.S. hackers. In the April 1, 2001, incident that triggered it, a Chinese fighter jet collided with a U.S. surveillance airplane over the South China Sea. China claimed that, starting on April 4, the U.S. hacker organization PoizonBOx then began attacking Chinese websites. Saying it acted to protect China, the HUC organized Chinese hackers for a self-defense attack starting on May 1, targeting U.S. websites. The U.S. hackers also fought back. The war lasted for seven days until the HUC announced an end to it on May 8. Chinese hackers used the "human-wave tactic" to bring the White House website down from 9 a.m. to 11 a.m. on May 4, 2001. [35]

In another famous hacker event targeting the U.S., hackers attacked *Cable News Network (CNN)*. In March 2008, Chinese media reported many stories claiming that CNN had aired malicious reports about China's suppression of Tibetans. This outraged the Chinese, especially when they were preparing for the upcoming Olympic Games, an event the Chinese media had been long promoting with national pride. Chinese hackers organized a DDOS attack against *CNN.com* starting April 19, 2008, and took it down for several days. [36]

In May and June 2011, after China and Vietnam exchanged heated words over the sovereignty of the South China Sea, Chinese hackers and Vietnamese hackers had a hacking war. Chinese media reported that Vietnamese hackers first broke into a Chinese website on June 2 and posted provocative messages such as "The Vietnamese people are willing to sacrifice to protect the sea, sky, and country!" Chinese hackers fought back using a "self-defense attack" on June 4 and 5 and claimed a landslide victory over the Vietnamese. [37] Over 1,000 Vietnamese websites were taken down. The HUC announced that it had taken down Vietnam's largest search engine for over 12 hours. [38]

While being a hacker is not ethically appealing, the Chinese hackers find comfort under the umbrella of "patriotism."

The HUC website claims it is "a non-governmental patriotic organization" and says, "All our words and actions are based on patriotism and safeguarding China's dignity. Our voices and actions are the manifestation of China's national integrity." [39]

Hacker Union of China is another prestigious hacker group in China. Its homepage displays a red slogan: "Safeguard the Nation's Dignity, Love Our China, Strengthen Our China, and Glorify Our China." [40]

Chinese hackers have claimed "love of country" as a motive in all of the mentioned hacker wars.

The "June 9 Holy War" event further exemplified the hackers' "patriotic" sentiment. It was triggered when Chinese fans of Super Junior, a South Korean pop group, clashed with Chinese armed police in Shanghai. Over 100,000 Chinese netizens participated in a "Holy War" to attack South Korea's government sites and company sites and any Chinese sites related to South Korea. Though the original conflict was between Chinese fans and Chinese armed police and no Super Junior member was involved, college students still call the attack a "patriotic event." [41]

The Government Connection

People's Daily interviewed Zhang Zhaozhong after the Chinese hackers' war with the U.S. hackers in May 2001. In his praise, Zhang stated, "Chinese hackers released their furor [about U.S. hegemony] and demonstrated their strong sense of mission, responsibility, and patriotism. Their motivation should be protected and praised…" [42]

Leaked cables from the U.S. State Department, as shown on *Wikileaks*, revealed that "the state department is concerned about Beijing's close working relationship with two major providers of information security in China. The companies have hired experienced hackers, who include Lin Yong, aka LION, who founded the Honker Union of China, a Chinese hacker group that emerged after the U.S. bombing of the Chinese embassy in Belgrade in 1999 and launched a series of cyber attacks on U.S. government-related websites." [43]

Nanfang Metropolitan Weekly, a Chinese publication based in Guangzhou, mentioned a junior-level hacker named "Renil." Renil was arrested and detained for over a month for hacking several Public Security Bureau's websites. After being released, he took a day job painting bridges, earning 60 yuan (US$9.37) a day. He spent his nights taking down foreign websites and was paid 1.5 yuan for each site he hacked. He made about 200 yuan (US$31.23) a night. The article did not mention who paid him for his hacking skills, but it would be worth investigating. [44]

A report from the *Journal of Strategic Security* stated, "Examples of cooperation between private hackers and the PLA do occur. Hackers have even publicly referred to their

incorporation into PLA operations in a 2005 message on the hacker community called the Honker Union of China. The message stated that the hackers have 'government-approved network technology security units.'" [45]

Since hackers are important to the PLA's cyberwarfare strategy, the hacker industry is allowed to exist in China. The National Computer Network Emergency Response Technical Team/Coordination Center of China estimated that the Chinese "hacker industry" received over 238 million yuan (US$36 million) in revenue in 2009. Even hacker training sites are common. [46]

There have been hacking incidents against human rights websites that criticize the CCP or call for democracy in China. In May 2011, *Boxun.com*, a U.S.-based human rights site was down for days due to a DDOS attack after articles on the site called for a Jasmine Revolution in China and listed the time and locations in different Chinese cities for holding protests. *Change.org*, which hosted a petition with over 100,000 signatures to free activist Ai Weiwei, was also taken down at the same time. [47]

III. The PLA in Action

Some experts believe that China has surpassed the United States in the cyberwar race.

1) The Cyberwar Blue Army

Senior Colonel Geng Yansheng, Director of the News Service Bureau, China's Ministry of Defense, revealed on May 25, 2011, that the PLA had established an "Online Blue Army," whose aim is to improve the level of security of the army's network. The notion of "blue army" comes from what is often referred as the "red-blue drill," in which the "blue army" usually plays the role of the opponent.

The "Online Blue Army," as the name suggests, is a network army built to have strength similar to the opposing Western network forces. Its strength is in its ability to conduct a cyberspace attack. It can simulate the level of an attack from the Western forces and thus be used to train the "Online Red Army," which will defend the network. This discussion also revealed that the "Online Red Army" already exited. [48]

Huanqiu quoted Hong Kong media, which reported, "The Ministry of Defense confirmed in May 2011 that a special cyber unit exists in every military command. China's military expert also said that many soldiers have received technical training on hacking and anti-hacking." [49]

Huanqiu also reported that the PLA has established its first cyberwar base. "It is officially called the Information Protection Base. This new military unit is under the General Staff Department. It will become the headquarters for all network strategic information centers in each military department or military command." [50]

Furthermore, out of a concern for security, "The PLA set rules that prohibit its 2.3 million soldiers from creating websites, setting up personal blogs, making friends online, or conducting online chat or online dating. They are not allowed to do so even if they are on vacation." [51]

2) Recruiting and Developing Warriors

Several U.S. reports stated that the PLA has recruited hackers to join its cyberwar army. On April 29, 2011, the *Washington Times* reported the following case in testimony to the U.S. Senate Committee on Homeland Security and Governmental Affairs. In 2005, the Chinese military recruited Tan Dailin, a graduate student from Sichuan University, after he won an annual hacker contest. The military put Tan through a 30-day, 16-hour-a-day training "where he learned to develop really high-end attacks and honed his skills." "By December, he was found inside [Defense Department] computers, well inside DoD computers." [52]

Financial Times reported that the PLA sponsors hacking competitions in universities and discussed Tang Zuoqi. Tang was "a lecturer at the College of Computer Science and Information at Guizhou University. According to his biography on the university's website he secured his job after winning prizes in a 2005 Internet warfare competition that the Chengdu military command held." [53]

An indirect reference is that the Chinese media frequently quote the U.S. intelligence community and DOD for recruiting hackers. The PLA uses this as justification for its practice. A *People's Daily Online* article reported that the U.S. National Security Agency and other federal government agencies plan to compete with private companies at the annual hacker conference Defcon in Las Vegas in 2011 in order to hire hacker talent. "In addition to the DOD, the Department of Homeland Security, and the National Aeronautics and Space Administration (NASA), several U.S. federal agencies will send headhunters to attend." [54]

3) Cyber-Espionage and Attack

Over the past several years, Western media have reported cyber-espionage and attacks that could be traced back to China. Though, for the most part, it is hard to prove

whether the PLA is behind these actions, the sophisticated break-in techniques used in these attacks "are generally beyond the capability of nongovernment hackers." [55]

Bloomberg reported that, according to a draft report by the U.S.-China Economic and Security Review Commission, computer hackers, possibly from the Chinese military, interfered with two U.S. government satellites four times in 2007 and 2008. "Such interference poses numerous potential threats, particularly if successful against satellites with more sensitive functions." "Access to a satellite's controls could allow an attacker to damage or destroy the satellite. An attacker could also deny or degrade as well as forge or otherwise manipulate the satellite's transmission." [56]

Reuters obtained secret U.S. State Department cables from *WikiLeaks* via a third party. They revealed that an Internet breach code-named "Byzantine Hades" was traced to the Chinese military. An April 2009 cable even pinpointed the attacks to a specific PLA unit. [57]

Huanqiu even reported on this *Reuter*'s article, stating, "The WikiLeaks cables and other U.S. government reports stressed that the Chinese hackers have completely conquered the U.S. government network system." [58]

In light of the acceleration of Chinese cyber-espionage, at a committee hearing on cyber-threats and national security, the chairman of the House Intelligence Committee, Mike Rogers (R-Michigan), called on the international community to take action to stop China's cyber-espionage. Rogers stated, "I don't believe that there is precedent in history for such a massive and sustained intelligence effort by a government to blatantly steal commercial data and intellectual property." [59]

In June 2011, Reuters reported that U.S. Defense Secretary Robert Gates said that Washington was seriously concerned about cyber-attacks and was prepared to use force against any it considered an act of war. [60]

Conclusion:

The PLA has long realized the significance of cyberwarfare. It takes it seriously, as this type of warfare offers a quick way for China to overcome U.S. superiority in warfare weaponry and techniques. The PLA has adopted the "People's War" (人民战争) strategy in the cyberwar arena, and it apparently is working for China. China now enjoys the upper hand in the cyberwar race and is conducting cyber-espionage and cyberattacks more and more frequently and openly.

Endnotes:

[1] *PLA Daily*, "Both Cyberwar and Nuclear Weapons Are Strategic Weapons; They Can Paralyze the World in a Second," December 24, 2009.
Republished by *Xinhua*: http://news.xinhuanet.com/mil/2009-12/24/content_12697203.htm.
[2] *PLA Daily Online*, "Cyberwar: Strategy Warfare in the Information Era," September 23, 2003.
http://www.chinamil.com.cn/item/newar/qydt/93.htm.
[3] *People's Daily Online*, "Who Can Win the Cyberwar? A Military Expert Comments on the Sino-U.S. Cyberwar," May 11, 2011
http://www.people.com.cn/GB/junshi/62/20010511/462008.html.
[4] *PLA Daily Online*, "After Opening the 'Pandora's Box of Cyberwar," March 10, 2011.
http://chn.chinamil.com.cn/xwpdxw/jskjxw/2011-03/10/content_4399689.htm.
[5] *Nanfang Weekend Online*, "How Strong Is China's Cyberwar Capability?" February 2, 2011.
http://www.infzm.com/content/24062.
[6] *PLA Daily Online*, "Cyberwar: Strategy Warfare in the Information Era," September 23, 2003.
http://www.chinamil.com.cn/item/newar/qydt/93.htm.
[7] *PLA Daily Online*, "Cyberwar: The Important Battlefield for Future Wars," August 10, 2009.
http://chn.chinamil.com.cn/xwpdxw/2009-08/10/content_4019954.htm.
[8] *PLA Daily Online*, "After Opening the 'Pandora' Box of Cyberwar," March 10, 2011.
http://chn.chinamil.com.cn/xwpdxw/jskjxw/2011-03/10/content_4399689.htm.
[9] *PLA Daily*, "Both Cyberwar and Nuclear Weapons Are Strategic Weapons; They Can Paralyze the World in a Second," December 24, 2009.
Republished by Xinhua, http://news.xinhuanet.com/mil/2009-12/24/content_12697203.htm.
[10] Chapter 5 "The New Methodology of War Games," *Unrestricted Warfare* by Qiao Liang and Wang Xiangsui, Beijing. Published by PLA Literature and Arts Publishing House, February 1999.
[11] *Xinhua*, "Discover the Truth Behind 'Cyberwarfare,'" August 14, 2009.
http://news.xinhuanet.com/herald/2009-08/14/content_11879554.htm.
[12] *Wikipedia*, "The People's War."
http://en.wikipedia.org/wiki/People%27s_war.
[13] *Huanqiu Online*, "Hong Kong Media: China's Cyberwar Army Applies Mao Zedong's War Tactics," August 4, 2011.
http://china.huanqiu.com/eyes_on_china/military/2011-08/1875446.html.

[14] *Nanfang Weekend Online*, "How Strong Is China's Cyberwar Capability?" February 2, 2011.
http://www.infzm.com/content/24062.
[15] *PLA Daily Online*, "Cyberwar: The Important Battlefield for Future Wars," August 10, 2009.
http://chn.chinamil.com.cn/xwpdxw/2009-08/10/content_4019954.htm.
[16] *Xinhua*, "Discover the Truth Behind 'Cyberwarfare,'" August 14, 2009.
http://news.xinhuanet.com/herald/2009-08/14/content_11879554.htm.
[17] *Huanqiu Online*, "Over Ninety Percent of Netizens Support China's Establishing a Cyberwar Command," June 29, 2009.
http://mil.huanqiu.com/china/2009-06/499958.html.
[18] *Huanqiu Online*, "Hong Kong Media: China's Cyberwar Army Applies Mao Zedong's War Tactics," August 4, 2011.
[19] *PLA Daily Online*, "Developing the War Capability Potential to Build a Cyberwar Army," May 10, 2001.
http://www.chinamil.com.cn/gb/jskj/2001/05/10/20010510017023_jsrdts.html.
[20] *Huanqiu Online*, "Over Ninety Percent of Netizens Support China in Establishing a Cyberwar Command," June 29, 2009.
http://mil.huanqiu.com/china/2009-06/499958.html.
[21] *PLA Daily Online*, "Suggestions on Building Cybermilitia Units," June 14, 2001.
http://www.chinamil.com.cn/gb/jskj/2001/06/14/20010614017049_jsrdts.html.
[22] *PLA Daily Online*, "Commenting on People Supporting a Battlefront," June 14, 2001.
http://www.chinamil.com.cn/gb/jskj/2001/05/14/20010514017053_jsrdts.html.
[23] *Financial Times Online*, "Chinese military mobilises cybermilitias," October 12, 2011.
http://www.ft.com/intl/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html#axzz1ab05wkit.
[24] Northrop Grumman Corporation, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Prepared for The US-China Economic and Security Review Commission," October 9, 2009.
http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.
[25] *Financial Times Online*, "Chinese military mobilises cybermilitias," October 12, 2011.
http://www.ft.com/intl/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html#axzz1ab05wkit.
[26] *PLA Daily Online*, "Military and Civilian Jointly Develop an 'Information Great Wall,'" July 4, 2001.
http://www.chinamil.com.cn/gb/pladaily/2001/07/04/20010704001165.html.

[27] *PLA Daily Online*, "Cybersecurity: The First Alarm of a Future Information War," December 19, 2000.
http://www.chinamil.com.cn/gb/jskj/2000/12/19/20001219002012_jsrdts.html.
[28] *Washington Times Online*, "China blocks U.S. from cyber warfare," May 12, 2009.
http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/.
[29] *China's Government Official Website*, "China's 'Tianhe-1 Becoming the World Fastest Super Computer," November 15, 2010.
http://www.gov.cn/jrzg/2010-11/15/content_1745540.htm.
[30] *DoDBuzz.com*, "China's ability to make quality jet engines," September 28, 2011.
http://www.dodbuzz.com/2011/09/28/chinas-ability-to-make-quality-jet-engines/.
[31] *Washington Times Online*, "Chinese telecom firm tied to spy ministry," October 11, 2011.
http://www.washingtontimes.com/news/2011/oct/11/chinese-telecom-firm-tied-to-spy-ministry/?page=all#pagebreak.
[32] *DoDBuzz.com*, "Report details defense industry cyber attack," November 1, 2011.
http://www.dodbuzz.com/2011/11/01/report-details-defense-industry-cyber-attack/.
[33] *People's Daily Online*, "Who Can Win the Cyberwar – Military Expert Comments on Sino-U.S. Cyberwar," May 11, 2011
http://www.people.com.cn/GB/junshi/62/20010511/462008.html.
[34] *Honker Union of China Website.*
http://baike.baidu.com/view/45832.htm.
[35] *Chinese Software Developer Network Website*, "China Hacker Record: Sino-U.S. Hacker War (1)," October 18, 2007.
http://news.csdn.net/n/20071018/109690.html.
[36] *eWeek*, "Chinese Hackers Knock SportsNetwork Offline; CNN.com Survives," April 21, 2008.
http://securitywatch.eweek.com/exploits_and_attacks/chinese_hackers_knock_sportsnetwork_offline_cnncom_survives_2.html.
[37] *Blogbus.com*, "Sino-Vietnam Hacker War."
http://dyughido.blogbus.com/logs/136515571.html.
[38] Government Website for Qidong City, Jiangsu Province, "Chinese Hacker's Counterattack Is a Great Success: Vietnamese Fell Apart and Asked the U.S. to Help," June 11, 2011.
http://bbs.qidong.gov.cn/read-htm-tid-171226.html.
[39] *Honker Union of China Website.*
http://baike.baidu.com/view/45832.htm.
[40] *Hacker Union of China Website.*
http://www.chinahacker.com/index.asp
[41] *Nanfang Weekly Online,* "Technology Ear – June 9 Holy War: Is It against South Korea or Just Commercial Hype?" June 22, 2010.

Republished by *Sina.com*: http://tech.sina.com.cn/i/2010-06-22/15534336612.shtml.
[42] *People's Daily Online*, "Who Can Win a Cyberwar – Military Expert Comments on Sino-U.S. Cyberwar," May 11, 2011
http://www.people.com.cn/GB/junshi/62/20010511/462008.html.
[43] *Guardian*, "WikiLeaks cables reveal fears over Chinese cyber warfare," December 4, 2010.
http://www.guardian.co.uk/world/2010/dec/04/wikileaks-cables-china-cyber-warfare.
[44] *Nanfang Weekly Online,* "Technology Ear – June 9 Holy War: Is It against South Korea or Just Commercial Hype?" June 22, 2010.
Republished by *Sina.com*: http://tech.sina.com.cn/i/2010-06-22/15534336612.shtml.
[45] *Journal of Strategic Security*, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," Volume IV Issue 2 2011.
http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss&sei-redir=1&referer=http%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26source%3Dweb%26cd%3D8%26ved%3D0CFIQFjAH%26url%3Dhttp%253A%252F%252Fscholarcommons.usf.edu%252Fcgi%252Fviewcontent.cgi%253Farticle%253D1101%2526context%253Djss%26rct%3Dj%26q%3Dchina%2520bounces%2520attacks%2520colleges%2520cyber%26ei%3DlSmJTvjVLs_PiAKDvYypDw%26usg%3DAFQjCNGHqpZE_QmzOwRUSQ9OPFwEeXev3g#search=%22china%20bounces%20attacks%20colleges%20cyber%22.
[46] *Xinhua*, "Investigation into China's Gray Industry of Hacker Business," June 12, 2009.
http://news.xinhuanet.com/herald/2009-06/12/content_11529888.htm.
[47] *The Dark Visitor*, "Shock: Chinese hackers not supporting the Jasmine Revolution," April 21, 2011.
http://www.thedarkvisitor.com/2011/04/shock-chinese-hackers-not-supporting-the-jasmine-revolution/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheDarkVisitor+%28T+h+e+-+D+a+r+k+-+V+i+s+i+t+o+r%29.
[48] *Beijing Daily Online*, "Chinese Cyber Army Shows Its True Face; Secrets of U.S., Japan, and Korea's Cyber Armies Revealed," May 29, 2011.
http://bjwb.bjd.com.cn/html/2011-05/29/content_406695.htm.
[49] *Huanqiu Online*, "Hong Kong Media: China's Cyberwar Army Applies Mao Zedong's War Tactics," August 4, 2011.
http://china.huanqiu.com/eyes_on_china/military/2011-08/1875446.html.
[50] *Huanqiu Online*, "Hong Kong Media Report PLA Established a Cyberwar Command," July 26, 2010.
http://military.people.com.cn/GB/42969/58519/12245120.html.
[51] Id.

[52] *Washington Times Online*, "China blocks U.S. from cyber warfare," May 12, 2009. http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/.
[53] *Financial Times Online*, "Chinese military mobilises cybermilitias," October 12, 2011. http://www.ft.com/intl/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html#axzz1ab05wkit.
[54] *People's Daily Online*, "U.S. National Security Agency Hires Hackers for 'Cyberwar,'" August 3, 2011. http://media.people.com.cn/GB/40606/15318340.html.
[55] *Washington Times Online*, "China blocks U.S. from cyber warfare," May 12, 2009. http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/.
[56] *Bloomberg*, "Chinese Military Suspected in Hacker Attacks on U.S. Satellites," October 27, 2011. http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html.
[57] *Reuters*, "Special report: In cyberspy vs. cyberspy, China has the edge," April 14, 2011. http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414.
[58] *Huanqiu Online*, "British Media: China Has an Upper Hand in Cyber-espionage," April 18, 2011. http://china.huanqiu.com/eyes_on_china/politics/2011-04/1634893.html.
[59] *Washington Post Online*, "Lawmaker calls for international pressure to stop China's cyber-espionage," October 4, 2011. http://www.washingtonpost.com/world/national-security/lawmaker-calls-for-international-pressure-to-stop-chinas-cyber-espionage/2011/10/04/gIQAAR26LL_story.html.
[60] *Reuters*, "China official says no cyber warfare between U.S., China," June 22, 2011. http://www.reuters.com/article/2011/06/22/us-china-us-cyberwar-idUSTRE75L1C520110622.