**Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies**
**The Bulletin of the Centre for East-West Cultural and Economic Studies**

Volume 8 | Issue 1 Article 2

October 2008

# How China will use cyber warfare to leapfrog in military competitiveness

Jason Fritz

Follow this and additional works at: http://epublications.bond.edu.au/cm

Recommended Citation
Fritz, Jason (2008) "How China will use cyber warfare to leapfrog in military competitiveness," *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*: Vol. 8: Iss. 1, Article 2.
Available at: http://epublications.bond.edu.au/cm/vol8/iss1/2

This Article is brought to you by the Centre for East-West Cultural and Economic Studies at ePublications@bond. It has been accepted for inclusion in Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies by an authorized administrator of ePublications@bond. For more information, please contact Bond University's Repository Coordinator.

# How China will use cyber warfare to leapfrog in military competitiveness

**Abstract**
Extract:

The People's Republic of China (PRC) may be a global power economically but its military lacks force projection beyond the Asia Pacific region. Its traditional military hardware is one to three generations behind the US and Russia. In light of these deficiencies it is probable that cyber warfare will provide China with an asymmetric advantage to deter aggression from stronger military powers as they catch up in traditional military capabilities. Cyber warfare would also allow China to leapfrog by means of technology transfer and exploiting adversary weaknesses. This investigation will address three primary questions: What is China's current military capability? How would cyber warfare allow China to seriously advance its strategic abilities? And what is the evidence that China is headed in a cyber warfare direction?

**Keywords**
cyber warfare, military, Chinese People's Liberation Army (PLA), defence budget, Internet, combat systems

This article is available in Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies:
http://epublications.bond.edu.au/cm/vol8/iss1/2

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

# HOW CHINA WILL USE CYBER WARFARE TO LEAPFROG IN MILITARY COMPETITIVENESS

*by Jason Fritz BS (St. Cloud), MIR (Bond)*

***Introduction***

*The People's Republic of China (PRC) may be a global power economically but its military lacks force projection beyond the Asia Pacific region. Its traditional military hardware is one to three generations behind the US and Russia. In light of these deficiencies it is probable that cyber warfare will provide China with an asymmetric advantage to deter aggression from stronger military powers as they catch up in traditional military capabilities. Cyber warfare would also allow China to leapfrog by means of technology transfer and exploiting adversary weaknesses. This investigation will address three primary questions: What is China's current military capability? How would cyber warfare allow China to seriously advance its strategic abilities? And what is the evidence that China is headed in a cyber warfare direction?*

## 1. Traditional Military Power of the PLA

In order to see how the Chinese military will 'leapfrog' in military competitiveness, it is necessary to establish its current capabilities. The Chinese People's Liberation Army (PLA) is composed of five main service branches, the PLA Ground Force, PLA Navy, PLA Air Force, Second Artillery Corps, and the PLA Reserved Force. China has one of the world's largest military forces, with 2.3 million active members, a reserve force of 800,000, and a paramilitary force of 3.9 million, for a grand total of approximately 7 million members. The PLA has tried to transform itself from a land based power, to a smaller, mobile, high tech power that is capable of reaching beyond its borders (Annual Report to Congress 2007; China's National Defense in 2006).

During the 1980's paramount leader Deng Xiaoping pushed for quality over quantity, and the military was reduced by one million members. In 1993, President Jiang Zemin officially announced a Revolution in Military Affairs (RMA) a part of the national military strategy for modernization. RMA is a theory about the future of warfare, often connected to technological and organizational recommendations for change in the United States military and others. RMA is tied to modern information, communications, space technology, and total systems integration. Careful observation of US involvement in the Kosovo, Afghanistan, and Iraqi wars, furthered China's interest in network-centric warfare and asymmetric warfare, the former successfully used by the US, and the latter successfully used against the US. At the turn of the century, the bulk of China's traditional military force remained 1950s to 1970s era technology imported and reverse engineered from Russia. China is seeking to modernize this force. The size of China's traditional force will shrink, as fewer numbers are needed when new technology is introduced (Cordesman and Kleiber 2006; Corpus 2006; Moore 2000).



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

China's defence budget has increased dramatically over the last 15 years. The official military budget of China was US$57 billion in 2008, making it the second largest military budget in the world. By contrast, the largest is the US with $623 billion, and the third largest is Russia with $50 billion. Japan, South Korea, and India are the next largest spenders in the Asia Pacific region with $41 billion, $21 billion, and $19 billion, respectively (World Wide Military Expenditures 2007). China's annual defence budget increases at approximately the same rate as its annual GDP, with an average increase of 9% per year since 1996 (Pike 2008; China's National Defense in 2006). However, China's total military spending may be far greater than the official figures reported. Foreign acquisitions, research and development of dual use science and technology, national security, construction, and emergency response and disaster relief, are a few examples of expenditures which may fall under non-military headings but directly relate to the advancement of the military. The US Department of Defence estimates China's total military-related spending for 2007 could be between $97 billion and $139 billion. Think tanks and academic institutions report a wide range of estimates for China's defence budget, using varying methodologies and sources, however most arrive at the same conclusion: China significantly under-reports its defence expenditures (Annual Report to Congress 2008; International Assessment and Strategy Center 2005).

**Ground Force**

The PLA Ground Force (PLAGF) is the world's largest, with 1.25 million personnel, or about 70% of the PLA's total manpower (Annual Report to Congress 2008). Approximately 400,000 of these troops are based in the three military regions (MRs) opposite Taiwan. According to the 2008 Military Balance of the International Institute for Strategic Studies (IISS), the PLAGF comprises 18 group armies which include 9 armoured divisions, 3 mechanised infantry divisions, 24 motorised infantry divisions, 15 infantry divisions, two amphibious assault divisions, one mechanised infantry brigade, 22 motorised infantry brigades, 12 armoured brigades, 7 artillery divisions, 14 artillery brigades, and nine anti-aircraft artillery missile brigades. China's military doctrine places an emphasis on electronic and information warfare, long-range precision strikes, surface-to-air missiles, special operations forces, army aviation helicopters, and satellite communications. The PLAGF continues to reduce its overall size, opting for a more high tech and mobile force (China's National Defense in 2006).

While much of the equipment remains antiquated, China is continually upgrading. This includes approximately 200 Type 98 and Type 99 main battle tanks now deployed to units in the Beijing and Shenyang MRs. As many as 6,000 tanks were produced by China in the 1960's. From the early 1970's to 2000, China's tank inventory remained around 10,000. This was mostly composed of old Soviet tanks and Chinese versions of old Soviet designs. China continually upgraded over the decades, but was always one step behind the current Soviet models. The Chinese-produced versions of the Soviet T-54A (Type 59 and Type 69) account for over two-thirds of the total PLA tank inventory. While retiring some of the older Type 59/69 series and replacing them with the second generation Type 88 and Type 96, the PLA is also upgrading the remaining Type 59/69 series tanks with new technologies including improved communication and fire-control systems, night vision equipment, explosive reactive armour, improved power plant, and gun-fired anti-tank missiles so that they can remain in service as mobile fire-support platforms. China's newest tank, the Type 99, entered PLA service in 2001. Maintenance of such a massive force becomes a problem, and many of China's tanks may have fallen into disrepair. This may also be a push for modernizing to a smaller but more effective force (Armoured Fighting Vehicles 2008).

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

The PLAGF's hand guns further illustrate China's attempts to modernize and catch up by means of foreign acquisition and reverse engineering. Most of China's weapons are derived from Soviet models acquired before the Sino-Soviet split in late 1950s and early 1960s. Examples include Soviet or Russian small arms like the Mosin-Nagant series rifles and carbines, the SKS carbine, the AK-47 assault rifle, the RPD light-machine gun, the Tokarev TT33 pistol, and the DShK heavy machine gun. The PLA's main infantry rifle, the QBZ-95 is derived from the Russian AK-47, and the Chinese Type 56 Assault Rifle is a direct copy, albeit locally produced and with a permanently attached bayonet with a more sword-like, stiletto style. The Chinese Type 56 Assault Rifle, a locally produced version of the SKS, also differs from its Russian counterpart by having a permanently attached bayonet. The Chinese Type 56 was mass produced from the 1960's to 1980's and was exported to many states around the world (Small Arms 2008).

**Navy**

The People's Liberation Army Navy (PLAN) is composed of 250,000 personnel divided into three major fleets, the North Sea Fleet, East Sea Fleet, and South Sea Fleet, each containing surface ships, submarines, naval air force, coastal defence, and marine units. China's naval force includes 57 attack submarines, 55 medium and heavy amphibious ships, and 49 coastal missile patrol craft. A priority has been placed on anti-air capabilities with improvements in over-the-horizon targeting, range, and accuracy in surface-to-air missiles. "Taking informationization as the goal and strategic focus in its modernization drive, the Navy gives high priority to the development of maritime information systems, and new-generation weaponry and equipment" (China's National Defense in 2006). As a part of PLAN's modernization program, PLAN has been developing blue water navy capabilities.

PLAN does not currently have an aircraft carrier. However, evidence suggests they are pursing such technology and have the capability to construct one. Renovation to a former Soviet Kuznetsov-class aircraft carrier may be used for training purposes, and the Chinese have expressed interest in acquiring Russian Su-33 carrier-borne fighters. The ex-Australian carrier Melbourne also provided research for the PLAN as it was towed to China for scrap. Russian assistance, coupled with an already capable ship building infrastructure, could allow PLAN to rapidly develop an aircraft carrier. The PLAN's ambitions include operating out to the first and second island chains, extending operations to the South Pacific near Australia, north to the Aleutian Islands, and west to the Strait of Malacca towards the Indian Ocean (Annual Report to Congress 2008).

China's submarine fleet is derived from outdated Russian technology and is seeking to become a more modern and smaller force. Early Chinese submarines were domestically produced versions of the Soviet Romeo class submarine, which were only capable of coastal patrols with deployment to sea limited to a few days per year. One Romeo was modified to carry six YJ-1 (C-801) anti-ship missiles, but it had to surface to fire them. The Chinese Ming class submarines produced in the 1970s were not much better, other than being of newer construction. This was followed by the Song class submarine, which had a streamlined hull and can be fitted with anti-ship missiles capable of being fired while submerged. China returned to purchasing subs in the late 1990s with the Russian Kilo class submarine. The Type 041 Yuan Class is the newest diesel-electric submarine in the PLAN. Its design incorporates parts of the Song class and Russian Kilo class submarines. The Yuan class has five torpedo tubes capable of launching indigenous torpedos as well as Russian



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

designed torpedos, and it is believed to have anti-ship missiles. This ship was designed to replace the aging Romeo and Ming class submarines which currently form the backbone of the PLAN's submarine fleet (Chinese Submarines 2008; see also China's Navy 2007).

Chinese produced Han class nuclear submarines were plagued with problems. A follow-on Type 093 nuclear submarine was developed with experience from the Han class and further assistance from Russian submarine builders, such as advanced wielding and construction techniques. Despite being armed with new Chinese wire-guided torpedoes; the Type 093's overall capability remains comparable to Russian technology of the late 1970s. Nevertheless, China continues to make progress and the true level of Russian assistance lacks transparency (Smith 2001). Further, the Type 093 may have benefited from German fuel cell technology and French design, which could allow for two to three weeks of submerged operations without having to surface to recharge batteries. Internet-source photos of Type 039s under construction also show Chinese mastery of advanced multi-layer rubber/polymer hull coatings that greatly reduce hull-radiated noise while limiting the effectiveness of active-sonar detection (Chinese Submarines 2008).

China maintains a fleet of approximately 28 destroyers, 48 frigates, and 30 ocean-capable fast attack craft. The frigates were designed for anti-surface warfare, and lacking significant self-defence. Chinese-built destroyers include the Luhu class, the Luhai class, and the Luda I/II/III, from oldest to newest, respectively. The Luhai and Luda class are armed with a battery of guns, torpedos, mortars, optional helicopter pads, and domestically built Crotale SAMs which were built from designs provided by France in the 1980s. Construction of the Luhai class was delayed from the mid 1980s to the mid 1990s due to construction of frigates for the Thai Navy. The most powerful addition to the PLAN is the Russian-built Sovremenny class destroyers. These include MOSKIT anti-ship missiles and KASHTAN combined gun/missile ship defence systems. While these designs are non-stealth 1970s Russian technology, outdated by current designs, they provided the PLAN with modern anti-ship, anti-air, and anti-submarine systems. The most recent Sovremenny acquisitions carry 8 Sunburn supersonic sea-skimming ASM and the SA-N-7 Gadfly, which will give PLAN limited naval air-defence capability. Up to this point, China only possessed short-range SAMs of French or domestic design (Surface Combatants 2008; IISS 2008).

Improvements in stealth design of the PLAN's ships further the notion that China seeks to modernize by purchasing or clandestinely obtaining technology from other states, reverse engineering that technology, and then attempting to make upgraded domestically produced versions. According to Frank Moore of the Institute for Defence and Disarmament Studies:

> The PLA developed new stealthy warships benefiting from Russian or Ukrainian design advice, weapons, electronics and other systems, plus new computer aided design methods which speeded their development. By 2002 it was possible to observe the construction of three new classes of warships via Chinese internet sources ... the No. 168 class, which armed with Russian SHTIL SAMs, Russian radar, Kamov Ka-28 ASW helicopters and Chinese C-802/803 anti-ship missiles, and powered by Ukrainian gas turbine engines. Soon after two No. 170 class destroyers were launched. These featured large phased array radar similar in appearance to the U.S. AEGIS system... Most likely the new "AEGIS" radar comes from the Ukrainian KVANT bureau and is a newly-developed active phased array radar with a broad search range of about 150km ... In 2003 [PLAN] launched two Type 054 stealthy frigates. Some sources indicate production was halted at two ships pending the completion of a new Russian SAM... In early 2004 internet-source pictures of a model of this new variant, apparently from a Chinese shipbuilding exhibition, confirmed that it will feature a new vertical-launched SAM and be outfitted with Russian radar and missile guidance systems. The Type 054 is also powered by co-produced French-designed SEMT Pielstick marine diesel engines.

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

> A fourth stealthy warship emerged in April 2004: a new fast-attack craft (FAC). Now being produced at two or three shipyards, this new FAC utilizes a wave-piercing catamaran (twin) hull design, which improves stability at high speeds even in rough seas. It is based on a design obtained from the Australian fast-ferry firm AMD... [with] radar-absorbing materials applied to the hull. (Moore 2000).

Not only does this illustrate China's use of foreign technology, it also demonstrates the complexity of modern warfare. These are highly sophisticated weapons, weapons pieced together from multiple sources, the existence of which was leaked onto the internet.

**Air Force**

The People's Liberation Army Air Force (PLAAF) is the third largest air force in the world behind the United States and Russia. The PLAAF employs 250,000 personnel and 1,762 combat aircraft (IISS 2008). The Soviet Union helped found the PLAAF in 1949, providing aircraft in 1951, and production technology and pilot training in 1953. China gained limited air combat experience during the Korean War. In 1956 China began assembling its own aircraft based on Soviet design, such as the J-2, J-5, and J-6, copies of the MiG-15, Mig-17, and Mig-19 respectively. The Sino-Soviet split was a significant setback to the PLAAF as was resource competition with the missile and nuclear divisions of the military. China's aircraft industry received a boost during the Vietnam War by providing aircraft for North Vietnam.

During the 1980s, the PLAAF underwent significant restructuring, opting for a more streamlined force and increased training. Due to the Sino-Soviet Split, the PLAAF turned to Western states for military expertise. Western states saw China as a counterbalance to the Soviet Union; however support dissolved following the 1989 Tiananmen Square incident. Reverse engineering of Soviet weaponry continued with the Chinese aircraft F-7 being an illegitimate copy of the MiG-21, and the F-8 incorporating various Soviet designs. Gorbachev's 1989 visit to China marked an end to the Sino-Soviet split. The newborn and economically struggling state of Russia used the transfer of military technology and expertise to China as a way to sustain its own aerospace industry (Moore 2000).

The collapse of The Soviet Union, and concerns over a Taiwan conflict that could draw in the United States, reinvigorated the PLAAF's modernization program. In the 1990s, China began development of fourth generation fighters, including the J-10 and a collaboration with Pakistan on the JF-17. China continued focusing on improved pilot training and retiring obsolete aircraft, preferring quality over quantity. The PLAAF is currently developing its own fifth generation stealth craft and increasing Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems for all its fighters.

In addition to jet fighter aircraft, "China is upgrading its B-6 bomber fleet (originally adapted from the Russian Tu-16) with a new variant which, when operational, will be armed with a new long-range cruise missile" (Annual Report to Congress 2008). China is also developing Airborne Early Warning and Control (AEW&C) aircraft utilizing Russian and possibly Israeli technology; and is making progress in tanker aircraft used for in-flight refuelling and airlift planes. These are important steps in obtaining the capability to conduct operations beyond China's borders (China's National Defense in 2006; Allen 2005).



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

Production of indigenous Chinese aircraft has been lacklustre. Most of the designs require foreign expertise which is then reverse engineered. The technology obtained is often one generation old at the time of acquisition, as states do not want to give up their advantage. Further, to reverse engineer they not only need the aircraft itself, but also high-precision and technologically advanced machine tools, electronics and components, skilled personnel, and facilities. By the time the technology is fully understood, and indigenous versions produced, the aircraft may be two or three generations behind the latest models of the world's advanced military forces. China is not alone in this difficulty. Except for the five largest industrial arms producers (France, Germany, Russia, the UK, and the US), other countries that have attempted to produce indigenously designed combat aircraft, such as Israel, South Africa, India, Taiwan, and South Korea, have abandoned their efforts and returned to importing systems from one of the five main producers. One reason is the economy of scale involved with financing research, development, and production of all of the systems and sub-systems that compose modern combat aircraft (Moore 2000; see also Allen, Krumel and Pollack 1995). Despite these difficulties, China remains committed to producing indigenous aircraft. Continued purchase of foreign technology demonstrates that the Chinese believe reverse engineering and then upgrading is the best approach to establish themselves as a self-sufficient producer in the future. In other words, the PRC aspires to become one of the elite weapons producers, but it does not want to wait for the infrastructure to evolve; it wants to leapfrog these capabilities.

**Space**

The PLA is responsible for the Chinese space program. China was the fifth nation in the world to place a satellite in orbit, the third nation to put a human into space, and the third nation to successfully test an anti-satellite weapon (ASAT) capable of destroying an enemy satellite in low earth orbit. China's manned space activities have received substantial support from Russia. This can be seen in the design of the Shenzhou spacecraft, which closely resembles the Russian Soyuz spacecraft. Although China's commercial space program has utility for non-military research, it also demonstrates space launch and control capabilities that have direct military application. All taikonauts have been selected from members of the PLAAF, and the PLA has deployed space-based systems for military purposes. These include imagery intelligence satellite systems such as the ZiYan series and JianBing series, synthetic aperture satellites (SAR) such as JianBing-5, the BeiDou satellite navigation network, and secured communication satellites such as FengHuo-1. China launched its 100th Long March series rocket in 2007, and continues to put more sophisticated and diverse satellites into orbit. The PRC is developing the Long March 5, an improved heavy-lift rocket that will be able to lift larger reconnaissance satellites into low-earth orbit or communications satellites into geosynchronous orbits by 2012. It expects to replace all foreign-produced satellites in its inventory with indigenously produced sun-synchronous and geo-stationary models by 2010 (Annual Report to Congress 2008; Center for Strategic and International Studies 2003).

Many of China's space assets are dual use, having financial and prestige benefits in addition to military applications. The Ziyuan-2 series, the Yaogan-1 and -2, the Haiyang-1B, the CBERS-1 and -2 satellites, and the Huanjing satellites, offer ocean surveillance, disaster and environmental monitoring, and high resolution imaging in the visible, infrared, and radar spectrums. New electro-optical satellites are capable of penetrating night and weather with a 1/10 meter resolution, providing near continuous targeting data for the PLA forces. In the arena of navigation and timing, China has five BeiDou satellites with 20 meter accuracy over

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

the region. The PRC also uses the Russian GLONASS navigation system and is a primary investor in the European Union's Galileo navigation system. China has developed small satellite design and production facilities, and is developing microsatellites, satellites which weigh less than 100 kilograms. These satellites offer remote sensing, imagery, and radar, and could allow China to rapidly replace or expand its satellite force in the event of war or a disruption to the network. The country is also improving its ability to track and identify foreign satellites, which is an essential component in the event of counter-space operations. China's successful test of an ASAT weapon demonstrates an ability to strike enemy assets in low earth orbit. This acts as a deterrent to conflict and demonstrates the PRC's commitment to relatively low-cost asymmetric warfare (International Assessment and Strategy Center 2005).

**Second Artillery Corps**

The Second Artillery Corps (SAC) controls the PLA's nuclear and conventional missile forces. Weapons from the SAC are subsequently filtered to other branches of the PLA. Items such as the land attack cruise missile (LACM) may be used by the PLAAF on H-6 bombers, or by the PLAN on Type 093 nuclear submarines. China's total nuclear arsenal is estimated to be between 120 and 250. China maintains a "no first use" policy; however, the ambiguous nature of declaratory policies leave open the option for first strike if China's leaders believe their national security or the CPC are under threat.

China began developing nuclear weapons in the late 1950s with the help of Soviet assistance. After the Sino-Soviet split in the late 1950s, China continued its development on its own and made significant progress. The People's Republic detonated its first atomic bomb in 1964, making it the fifth state to do so, following the United States, Russia, the United Kingdom, and France. With the addition of India and Pakistan, and possibly Israel and North Korea, China remains only one of nine states with a nuclear capability. China launched its first nuclear missile in 1966, and detonated its first hydrogen bomb in 1967. Short-range ballistic missile (SRBM) capability was obtained with the development of the Dongfeng-1, medium-range ballistic missile (MRBM) capability with the Dongfeng-2, intermediate-range ballistic missile (IRBM) capability with the Dongfeng-3, and limited intercontinental ballistic missile (ICBM) capability with the Dongfeng-5 (Missile and Space Programme 2008; Second Artillery Corps 2000).

It is estimated that China has 24-36 liquid fuelled ICBMs capable of striking the US and approximately 100-150 IRBMs capable of striking Russia and Eastern Europe. China also possesses approximately 1,000 SRBMs with ranges between 300 and 600 km. Beijing is continually upgrading the range, accuracy, and payload capability of its SRBMs at a rate of 100 new missiles per year. Its most current missile, the Dongfeng-31A is a solid fuel ICBM with a range of 11,200km. It is road mobile, and has multiple independently targetable re-entry vehicles (MIRVs). As noted above, China possesses submarine-launched ballistic missiles (SLBMs) on its SSBN submarines. The PLAAF also has bombers capable of delivering nuclear bombs. However, they would be unlikely to break through the modern air defence systems of advanced military powers. The SAC has sought to improve its retaliatory strike capability by hardening missile silos, developing mobile launchers, and increasing range, accuracy, and response time of its missile system (Annual Report to Congress 2008; see also Wortzel 2007).



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

China's non-nuclear missile arsenal continues to develop anti-access/area denial capabilities. These include the land attack cruise missile (LACM) DH-10, the Russian SUNBURN anti-ship cruise missile (ASCM), the Russian SIZZLER supersonic ASCM, and indigenous versions of anti-ship missiles based on their own MRBMs. The acquisition of Russian arms demonstrates China's continued commitment to technology transfer and reverse engineering. Thus, "The DH-10 will be similar in size and capability to the U.S. TOMOHAWK, in part because the PLA has been collecting parts of this U.S. cruise missile from Iraq and Afghanistan. The PLA has obtained at least six Russian Kh-55 cruise missiles from the Ukraine, and reportedly, has benefited from Israeli cruise missile technology associated with the DELILAH anti-radar missile" (Moore 2000). Asymmetric warfare, another tendency of the PLA, is shown by its research into manoeuvring re-entry vehicles (MaRV), decoys, chaff, jamming, thermal shielding, and ASAT weapons that will strengthen deterrence and strike capabilities. Many of these technologies can also be used to defeat, deter, or stymie US attempts at a National Missile Defence shield. By examining the weapons and deployment of the SAC, China's perceived primary threats can be identified. The majority of the SAC's SRBMs are opposite Taiwan. DF-11 Mod 1s are capable of carrying thermobaric and cluster munitions as well as high-explosives. In addition, they may carry radio-frequency/electromagnetic pulse (EMP) warheads which, if used in sufficient numbers, could disable electronic communications and electric power networks (Annual Report to Congress 2008).

**People's Armed Police**

The People's Armed Police (PAP) is no longer the official fifth service branch of the PLA; however it remains an integral part of Chinese defence. The line between military operations against foreign elements and operations of internal security are often blurred. This can be seen all the way down to the PAP uniforms which differ only slightly from PLAGF, often leading foreigners to mistake them as soldiers. In contrast, public security officers wear dark gray or blue uniforms more common among Western police forces. Much of the PAP force was absorbed directly from the PLA. They use a similar rank structure, and they obey the PLA's general regulations. PAP guards are also recruited at the same time and through the same procedures as PLA soldiers. The PAP has a dual command structure including the Central Military Commission (CMC) and the State Council through the Ministry of Public Security. By law the PAP is not part of the PLA; however, their interconnection is unavoidable, and the PAP will play an important role as domestic or non-military issues become intertwined with traditional military issues (People's Armed Police Force Organisation 2007; Tkacik 2007).

The PAP is a paramilitary force primarily responsible for law enforcement. China's National Defence White Paper, published in 2006, lists the total strength of the PAP at 660,000. The IISS Military Balance of 2008 lists an estimated 1.5 million (IISS 2008). The PAP has its origins in the PLA, which was originally tasked with both defending China from foreign threats and providing internal security. While the two share much in common, China eventually decided the differences were greater than the similarities. The PAP's primary mission is internal security. They are responsible for guarding government buildings at all levels, including party and state organisations, foreign embassies, consulates, and airports. The PAP provides personal protection to senior government officials, and performs security functions for major corporations and public events – including its much-publicized role in the 2008 Beijing Olympics (see Paramilitary Olympics 2008). Additionally, the PAP maintains multiple counter-terrorism units, sea and land border security forces, fire fighting units, and

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

has a role in the protection of forests, gold mines, hydroelectric facilities, and highway infrastructure. The secondary mission of the PAP is external defence, and in times of war PAP internal security units can act as light infantry supporting the PLA in local defence missions. Similarly, the PLA can fill in for the PAP and has done so during the Cultural Revolution, the Tiananmen Square incident, and flooding of the Yellow River (People's Armed Police Force Organisation 2007; China's National Defense in 2006; People's Armed Police 2005).

**Military Intelligence**

The General Staff Department carries out staff and operational functions for the PLA and is responsible for implementing military modernization plans. It serves as the headquarters for the PLAGF and contains directorates for the PLAN, PLAAF, and SAC, as well as a department for electronic warfare. The General Staff Department also includes sub-departments for artillery, armoured units, communications, engineering, mobilization, operations, politics, training, and surveying. Direct control over the four military branches is sub-divided among the General Staff Department and regional commanders; however the General Staff Department can assume direct operation control at any time. The General Staff Department is under the control of the Central Military Commission (General Staff Department 1997).

The Second Department of the General Staff Headquarters is responsible for collecting military intelligence. This includes military attachés at Chinese embassies abroad, clandestine agents to conduct espionage, and the analysis of publicly available data published by foreign countries. The Second Department oversees military human intelligence (HUMINT), open source intelligence (OSINT), and satellite and aerial imagery intelligence (IMINT) which it disseminates to the Central Military Commission and various branches. The Second Department has increased its focus on scientific and technological military intelligence gathering. The Third Department of the General Staff Headquarters is responsible for monitoring the telecommunications of foreign militaries and producing reports based on the military information gathered. China operates the most extensive signals intelligence (SIGINT) network of all the countries in the Asia-Pacific region. Since the 1950s, the Second and Third Departments have maintained a number of secondary and higher learning institutions for producing recruits, particularly in foreign languages. The Third Department not only intercepts communication of foreign militaries, but also those of the PLA, thereby maintaining control and supervision over the different branches and commanders within all of the military regions (Second Intelligence Department 2005, General Staff Department 1997).

Other branches of the General Staff Department include the Fourth Department and the General Political Department (GPD). The Fourth Department (ECM and Radar) is responsible for electronic intelligence (ELINT) including electronic countermeasures and maintaining databases on electronic signals. The GPD is responsible for overseeing the political education required for advancement within the PLA and controls the PLA's internal prison system. The International Liaison Department, a branch within the GPD, conducts propaganda, psychological operations (PSYOPS), and counter-espionage against foreign intelligence. As with the PAP, many of the departments within the General Staff Department appear to have significant overlap. The structural details are beyond the scope of this study; however, they are worth noting, as they pertain to the discussion below of cyber warfare.



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

**Technology Transfer**

China continues to pursue the acquisition of foreign military technology. Beijing is in ongoing negotiations with Moscow to obtain multiple weapons systems, and in 2007 signed arms agreements worth $150 million. Israel has previously supplied advanced military technology to China. However, under pressure from the US, Israel began to implement strict military export regulations. China is attempting to remove an embargo placed on lethal military export from the EU. This embargo was a response to the Tiananmen Square incident. Opinion on removing the embargo remains divided among EU member states. According to the 2008 Annual Report to Congress on China's Military:

> China continues a systematic effort to obtain dual-use and military technologies from abroad through legal and illegal commercial transactions. Many dual-use technologies, such as software, integrated circuits, computers, electronics, semiconductors, telecommunications, and information security systems, are vital for the PLA's transformation into an information-based, network-enabled force.

Between 1995 and 2008, several high profile cases of Chinese espionage against the US surfaced. These attempts targeted aerospace programs, space shuttle design, F-16 design, submarine propulsion, C4ISR data, high-performance computers, nuclear weapons design, cruise missile data, semiconductors, integrated circuit design, and details of US arms sales to Taiwan. Targeted organisations include Northrop Grumman, NASA, Los Alamos Laboratories, Boeing, Lockheed Martin, Sun Microsystems, and various defence installations. The Chinese do not limit themselves to high value targets or an elite group of agents. They obtain any data which may be of value, including legally obtained documents or OSINT, which may help them piece together the larger picture. China utilizes a decentralized network of students, business people, scientists, diplomats, and engineers from within the Chinese Diaspora. The majority of these individuals have legitimate purposes within the host state; however they are recruited at a later date, or asked for small pieces of information or favours which can seem harmless in scope to the individual. Attempts are also made to purchase interests within high technology companies, as well as win political favour with government officials. For example, there have been repeated allegations that President Bill Clinton's decision to sell sophisticated computer and satellite technology to China was influenced by campaign contributions (Appel 2004; Cooper 2006; Grier 2005; Jordan 2008; Warrick and Johnson 2008; Lynch 2007; Cox Report 1999; McLaughlin 1999; PRC Acquisitions of US Technology 1998).

China's use of espionage to obtain foreign military technology is not restricted to the US. In 2007, the head of a Russian rocket and space technology company was sentenced to 11 years for passing sensitive information to China. An alleged agent who defected in Belgium claimed hundreds of Chinese spies were working within Europe's industries. These allegations coincided with an arrest in France for illegal database intrusion of the automotive components manufacturer Valeo, and a guest researcher in Sweden arrested for stealing unpublished and unpatented research. Further, Chinese diplomat Chen Yonglin defected to Australia in 2005, claiming there were over 1,000 Chinese secret agents and informants within Australia (Luard 2005; Isachenkov 2007). Espionage and technology transfer prosper in cyber warfare, where being physically present is not required, and attribution becomes increasingly difficult. It also falls in line with China's strategy of leapfrogging. By acquiring foreign military knowledge, China can quickly catch up and begin working at a comparable level, rather than investing the large amounts of time and effort it would take to acquire this knowledge independently.

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

**Doctrine/Strategy**

Chinese military doctrine and strategy remain focused on modernization. Beijing has not explicitly laid out an official grand strategy. This may be due to disagreement within the government, or done intentionally to hide true motives and avoid being bound by them. Much of the writings published by the PRC are contradictory or ambiguous, using modern and ancient foundations, while being disseminated by varied sources. However, several points which are continually emphasized may point to a general consensus. These include modernization of weapons, equipment and training; accelerating the RMA; improving education and training of the PLA and the CPC; "informationized" (*xinxihua*) warfare; and scientific development. China seeks to maintain domestic and regional stability while developing its economic, military, technologic, scientific, and soft power. It also seeks a balance between military and economic development, believing they are mutually dependant. Beijing maintains its One China Policy in relation to Taiwan, and claims sovereignty over the Parcel and Spratly islands and adjacent waterways (China's National Defense 2006).

Deng Xiaoping, representing second generation leadership after Mao, sought to avoid international responsibilities and limitations, as they could slow down development of the military and economy. The third generation leadership of Jiang Zemin did look outward, promoting a multipolar world in the face of the post-Cold War unipolarity under the US, just as fourth generation leader Hu Jintao promoted the ideology of a Harmonious World *(hexie shijie)* which places more emphasis on international relations (Lam 2004; Zheng and Tok 2007). However the PRC continues to avoid concrete stances through concepts of non-interference, diversity, and equality. It compares itself to other states through Comprehensive National Power (CNP - *zonghe guoli*), using qualitative and quantitative values, and not accepting traditional Western categorizations (see Pillsbury 2000). For example, China includes the economy, soft power, and domestic stability as factors of CNP. This is important, because it shows a correlativity which holds relevance for cyber warfare. Under CNP the economy, soft power, and domestic stability can be seen as military matters. Further, maintaining the status quo in regards to Taiwan and the Spratly islands may not be China's long-term intention, but rather a way to stall efforts while it builds up military strength, strength which can include economic and international influence.

Despite not wanting to become embroiled in concrete commitments to military strategy, Chinese leaders cannot ignore the interconnectedness of the modern world, and they have realized the necessity of international cooperation. For example, the need for resources has fuelled China's global presence. The PRC is the world's second largest importer of petroleum. As the country's economy grows and the middle class expands, the demand for fossil fuel resources will continue to grow. This creates a need for sound international relations with exporting nations and the need for securing transportation routes, such as the Strait of Malacca and the South China Sea. These are intertwined with the politics and military affairs of the states involved. Competition with the US for these resources has often led to China making agreements with nations the US opposes on several points, such as Angola, Chad, Egypt, Indonesia, Iran, Kazakhstan, Nigeria, Oman, Saudi Arabia, Sudan, Venezuela, and Yemen (Hanson 2008; Brookes 2006).

Beijing may be using these countries simply because there is less competition for resource access in the case of these suppliers. However, the result is often international criticism of China as these states may be violating human rights or supporting terrorism. Moreover,



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

Beijing's methods of befriending these exporters comes into question, especially in regards to arms being traded or availability of finance which may be supporting controversial policies. China currently lacks the power projection to protect critical sea lanes from disruption or to deter international criticism. Crucial to extended power projection is the blue water navy which would benefit from online technology transfer and the further development of C4ISR. Online PSYOPS and media warfare would enhance China's soft power. Beijing believes that economic growth is critical to military development; economic growth creates a greater energy demand, which in turns creates a greater military demand, thus the two form a positive feedback loop (Ikenberry 2008; China's National Defense in 2006).

While Beijing recognizes the need for international cooperation, it remains cautious. The country suffered greatly from foreign incursions within the last century. Colonialism by Western powers, Japanese occupation in World War II, the Korean War, the Vietnam War, and border conflicts with India, the Soviet Union, and Vietnam are all kept fresh through China's historical discourse. Despite China's long history, these events are of special note as they are within living memory, and these events were present during the founding and duration of the CPC's rule.

Ensuring the survival of the CPC shapes China's strategic outlook. In order to bolster domestic support for policies, nationalism has been emphasized over communist ideology. This can be seen with government organised protests against Japan over visits by Japanese leaders to WWII war shrines and protests against the publishing of Japanese school text books which downplay Japan's atrocities against the Chinese. These protests often coincide with other strategic interests, such as territorial disputes in the East China Sea, which are often unbeknownst to the casual observer or participant. The mobilization of nationalism can also be seen during the holding of a US reconnaissance plane in 2001, and the mistaken bombing of the Chinese Embassy in Belgrade in 1999. The 2008 Olympics further demonstrated how China could garner national support in the face of a widening wealth gap, forced relocation, corruption, and environmental degradation. These events demonstrate a strategic value in public manipulation through nationalism; one that is interconnected with military affairs, and one which is increasingly turning to online assets (see Faiola 2005).

Several conclusions can be drawn from the status of the PLA. China is committed to modernizing its military, primarily through the purchase or illicit acquisition of foreign technology and subsequently reverse engineering that technology so it can be produced domestically. The PLA has placed an importance on trimming down its size, favouring quality over quantity. The PLA's weaponry often lags one or two generations behind that of Western military powers. However, the total force base still poses a significant deterrent, and establishes China as a dominant power within the Asia-Pacific Region. China lacks force projection beyond its region, primarily do to the lack of a blue water navy and aircraft carrier fleet, but also due to limits in missile technology and air-defence penetration, and opposition by foreign powers such as the United States. China seeks to become self-sufficient in many of these key capabilities. Once they have leapfrogged and are no longer trying to catch up, the Chinese will no longer need such widescale technology transfer, and they will possess the might to shape the international system, rather than be bound by one that was created by foreign powers.

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

## 2. A New Era

History has demonstrated that the advantage often goes to those who develop a technology first. The great naval voyages of Ming admiral Zhang He were unprecedented for their time and helped establish China as a suzerain of the wider Asian region. However, the mid-15th century saw China retreat to xenophobic and isolationist policies that paved the way towards China's decline and opened the door for colonialism (see Dick 2006). This lesson has not been lost among Chinese officials, and it is often used to spur initiatives such as their stated desire to be the first to mine the moon for helium-3 (China's Space Program 2005). The information revolution has given more power to individuals and increased globalization through the interconnectedness of economies, rapid dissemination of news, and improved access to communication and information of all types. Any attempt to compete on a global level without the use of these technologies would place the PRC at a significant military and financial disadvantage. For this reason, the benefits of electronic reliance outweigh the risks involved. Further, it is impossible for a state to develop a defence against cyber warfare without simultaneously learning how to execute attacks themselves.

The US is the sole superpower, making it a benchmark for military competitiveness. Beijing also views the US as a potential adversary, in particular due to perceptions of the US military attempting to encircle China with bases in nearby states and opposition to China's modernization goals, to concerns over any forceful application of the One China Policy, and to concerns over a range of internal affairs issues. China seeks to learn from US mistakes and successes, using American expertise and field-tested military experience to accelerate China's development. The People's Republic also focuses on weaknesses in the US military in order to improve upon the American example and to expose asymmetric advantages. For these reasons it is important to examine where the US is headed in military thinking and development, as China is likely to follow (Derene 2008; Lasker 2005; Liang Xiangsui 1999).

### Network-Centric Warfare

The US has viewed the internet as a potential tool of warfare since its inception. Arpanet, a precursor of modern internet, was heavily funded by the US military, with a particular emphasis on its research collaboration benefits. Despite fears of cyber terrorism post 9/11, the US continues to place increasing reliance on the internet as a security tool. This can be seen in the restructuring of US intelligence agencies and the creation of new online exchange such as Intellipedia and A-Space (Shaughnessy 2008; Magnuson 2006). Militarily, the information revolution has given rise to an increasing reliance on situational awareness, weather monitoring, surveillance, communication, and precision strikes. Chinese military strategists have made special note of the US reliance on, and dominance with, electronic means in the Kosovo, Afghanistan, and Iraqi conflicts (Tellis 2007; Center for Strategic and International Studies 2003; Liang and Xiangsui 1999).

Since the 1990s the US has put emphasis on developing network-centric warfare (NCW). NCW seeks to translate an information advantage, enabled in part by information technology, into a military advantage through the networking of well informed, geographically-dispersed forces. Originally described as a system of systems, it includes intelligence sensors, command and control systems, and precision weapons that enable enhanced situational awareness, rapid target assessment, and distributed weapon assignment. In essence, NCW translates to information superiority, which requires the reduction of hard categorization, because compartmentalizing military branches can stem the flow of information. In 2001, the

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

Pentagon began investing in peer-to-peer software as a means to spread information while supplying redundancy and robustness. The US Department of Defense has sought the creation of the Global Information Grid (GIG) as a backbone of NCW. All advanced weapons platforms, sensor systems, and command and control centres are eventually to be linked via the GIG. Collecting, processing, storing, disseminating, and managing classified security information on demand will be made globally available to soldiers, policymakers, and support personnel to achieve information superiority (Alberts 2002; Alberts, Garstka, and Stein 2000).

Vice President Richard Cheney stated in 2004:

> With less than half of the ground forces and two-thirds of the military aircraft used 12 years ago in Desert Storm, we have achieved a far more difficult objective . . . . In Desert Storm, it usually took up to two days for target planners to get a photo of a target, confirm its coordinates, plan the mission, and deliver it to the bomber crew. Now we have near real-time imaging of targets with photos and coordinates transmitted by e-mail to aircraft already in flight. In Desert Storm, battalion, brigade, and division commanders had to rely on maps, grease pencils, and radio reports to track the movements of our forces. Today, our commanders have a real-time display of our armed forces on their computer screen (Raduege 2004).

**Information Operations**

In 2003, under the direction of former Secretary of Defense Donald Rumsfeld, the US expanded on NCW in a document titled the *Information Operations Roadmap*. Now declassified, it was obtained under the Freedom of Information Act by George Washington University's National Security Archive. Information Operations (IO) calls for NCW to become a core military branch along with the Army, Navy, Air Force, Intelligence, and Space. To accomplish this it requires the development of a comprehensive education program to enlist new recruits, and an overhaul of the organizational structure of current military branches in an attempt to break down barriers that hinder information exchange and progress. IO activities include PSYOPS troops who try to manipulate the adversary's thoughts and beliefs, military deception and disinformation, media warfare, electronic warfare (EW), and computer network operations (CNO). Thus Information Operations Roadmap stands as an another example of the US commitment to transform military capabilities to keep pace with emerging threats and to exploit new opportunities afforded by innovation and rapidly developing information technologies.

IO seeks to "dominate the electromagnetic spectrum", in an attempt to "deny, degrade, disrupt, or destroy a broad range of adversary threats, sensors, command and control and critical support infrastructures" (Information Operations Roadmap 2003). The document notes that PSYOPS and manipulating the thoughts of populations through media and internet require constant observation during peacetime, otherwise in the event of conflict, a state would not be sufficiently engrained into the information culture to utilize them fully. This can be seen with the emergence of patriotic hackers, the advancement of social media, and the rapid evolution of memetics, slang, and subcultures, all of which will be discussed further below (List of Internet Phenomenon 2008; Pang 2008; Slashdot Subculture 2008; Slashdot Trolling Phenomenon 2008). IO includes defence, attack, and reconnaissance as vital components (Information Operations Roadmap 2003).

IO seeks to put out a political message in coordination with any traditional military assault. It places an emphasis on finding, and clandestinely promoting, favourable media from third

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

parties, so as to appear more credible. IO also seeks to establish a legal framework to defend against cyber attacks and cyber reconnaissance, as well as establish rules of engagement for conducting cyber attack. For example, how much certainty is required in identifying the source of an attack before responding? If an attack is being routed through multiple computers, is it acceptable to attack the intermediary computer? This would halt the attack but it would harm or destroy a computer which may have been infected without the owner's knowledge or consent. Additionally, an intangible computer attack can result in significant tangible loss, but does this warrant the use of traditional military weapons as a response?

**Future Combat Systems**

Another US project that is gaining attention and closely resembles NCW and IO is Future Combat Systems (FCS). FCS places a particular emphasis on advanced robotics, including Unmanned Ground Vehicles (UGVs), Unmanned Aerial Combat Vehicles (UCAVs), Non-Line of Sight Launch Systems, and Unattended Systems. This system of systems seeks to make warfare as networked as the internet, as mobile as a mobile phone, and as intuitive as a video game. The highly interconnected nature of FCS can even be seen in its development, utilizing 550 contractors in 41 US states. While the US has yet to determine a definitive name for this new type of information based, highly networked, and highly technological warfare, it is clear that the US government has spent a significant amount of time and money seeking to make it a reality. US Army officials have already stated that they intent to change FCS's name, because they believe the name is inappropriate, stating 'the future is now' (FCS Watch 2008; Future Combat Systems 2008; Baard 2007; Klein 2007; Gannon 2001).

Some of the complex logistical problems inherent in such an undertaking include: finance allocation, giving the approval for use to commanders, inter-agency cooperation, a common vernacular, rules of engagement, and adhering to the program's stated goals. The US is continually modernizing its cyber force, creating new hacker units, conducting cyber war exercises, and diversifying and limiting the number of access points that could be used for an attack (Waterman 2008; Greenberg 2007). And the US is not alone, 'more than 120 countries already have or are developing such computer attack capabilities' (GOA 1996). Information warfare is being adopted by all modern nations and competition is mounting.

**Informationization**

China's 2006 white paper on national defence places an emphasis on the informationization of the military. "Informationization" (*xinxihua*) means improving the PLA's ability to use the latest technologies in command, intelligence, training, and weapon systems. New automatic command systems linked by fibre-optic internet, satellite and new high-frequency digital radio systems, allow for more efficient joint-service planning and command, while also enabling a reduction in layers of command. The PLA's move towards information technology can be seen with the use of new space-based surveillance and intelligence gathering systems, ASATs, anti-radar, infrared decoys, and false target generators. PLA soldiers are using decision simulators, a low-light automatic tracking system for helicopters, and a battlefield artillery/mortar fuse jamming system derived from Russian technology. OSINT on China's military continually makes note of informationization and the related, if not identical, fields of cyber warfare, information warfare, CNO, and EW. "Priority is given to R&D of new and high-tech weaponry and equipment, and endeavours to achieve breakthroughs in a number of key technologies and leapfrogging technological progress, thus speeding up weaponry and equipment modernization" (China's National Defense 2006).



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

Informationization includes increased education of soldiers in cyber warfare and NCW, a reorganization of military branches and command system, and integrating joint operations. The PLA is improving the information network for military training, and has built more virtual laboratories, digital libraries and digital campuses to provide distance learning and online teaching and training. University courses have emerged for cyber attack and defence, a study of hacker methods, computer virus design and application, and network security protocols (Annual Report to Congress 2008). Following the Russian example, China is engaging in the debate of defining cyber warfare, in part through the Shanghai Cooperation Organization, in order to have a hand in the shaping of a legal framework and rules of engagement related to this new warfare. The PLA is pursuing a comprehensive transformation from a mass army designed for protracted wars of attrition on its territory to one capable of fighting and winning short duration, high intensity conflicts along its periphery against high-tech adversaries (Annual Report to Congress 2008) – an approach that China refers to as preparing for "local wars under conditions of informationization" (China's National Defense 2006).

**Exponential Growth and Unrestricted Warfare**

One view on twentieth century patterns of unrestricted warfare has noted:

> The names Watt and Edison are nearly synonymous with great technical inventions, and using these great technological masters to name their age may be said to be reasonable. However, from then on, the situation changed, and the countless and varied technological discoveries of the past 100 years or so makes it difficult for the appearance of any new technology to take on any self importance in the realm of human life. While it may be said that the formulations of "the age of the steam engine" and "the age of electrification" can be said to be names which reflect the realities of the time, today, with all kinds of new technology continuously beating against the banks of the age so that people scarcely have the time to accord them brief acclaim while being overwhelmed by an even higher and newer wave of technology, the age in which an era could be named for a single new technology or a single inventor has become a thing of the past. This is the reason why, if one calls the current era the "nuclear age" or the "information age," it will still give people the impression that you are using one aspect to typify the whole situation. (Qiao Liang & Wang Xiangsui 1999).

It is important to stop for a moment and ponder the rapid advancement in military weaponry. New weaponry and concepts are easily dismissed as science fiction, yet the integration of mobile phones and the internet in 2008 would resemble science fiction to someone in the 1980s. Reports of research and development may be noted momentarily before being subsumed in a busy, informationally-competitive world. For the purpose of this study, it is useful to acknowledge them in passing as they show the rapid advancement in science and technology, where military weapons are headed, and the increasing complexity and cooperation involved in their development and use. Current militarily-applicable science and technology, under development or already in use, include: augmented reality (Bonsor 2008); biotechnology; genetics; giving soldiers internal/biologic infrared, night vision, radar, and sonar capability (Block 2006); GPS; force fields (Hershkovitch 1998); invisibility cloaks (Mark 2008; Winkler 2003); microwave guns (Beam It Right There Scotty 2005); nanotechnology; neuroscience; positron bombs (Davidson 2004); robotic exoskeletons (Berkeley Bionics Human Exoskeleton 2007; Yeates 2007); space-based weapons such as ANGELS (Lewis 2005) and Rods from God (Adams 2004); telepathy (Braukus 2004; Put Your Mobile Where Your Mouth Is 2002); thought control of internet surfing and electronic

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

devices (New Technology Operated by Thought 2007); unmanned ground combat vehicles (Bloom 2008); and unmanned combat aerial vehicles (Pike 2008).

Adding further to this complexity, *Unrestricted Warfare*, a book by two PLA senior colonels, Qiao Liang and Wang Xiangsui, claims that warfare is no longer strictly a military operation, and that the battlefield no longer has boundaries. *Unrestricted Warfare* was published by the PLA Literature and Arts Publishing House in Beijing in February 1999. According to the FBIS translation editor, the book 'was endorsed by at least some elements of the PLA leadership' and an interview with one of the authors was published in the CPC Youth League's official daily newspaper on June 28, 1999. Thus while the book is not entirely backed by the PLA, especially the older generation, like the 'half empty, half full' glass analogy, it does have some official backing and hence a degree of legitimacy as a document assisting analysis as to where the PLA is headed and how asymmetric tactics against a superior hi-tech military might be employed.

Environmental concerns, human rights in regard to weapons of mass destruction, and the increasingly intertwined economies and political structures of globalization all have an impact on modern warfare. Sheer might of weaponry can no longer guarantee victory under these conditions. US extravagance in weaponry has been shown to stymie in the face of guerrilla warfare in Vietnam and Iraq. Under limited warfare, asymmetric warfare has seen a resurgence in use and value. Terrorist groups such as Al Qaeda employ guerrilla tactics and make use of the internet and financial institutions to subvert traditional warfare (Levinson 2008; Yassin 2008). No single weapon can deliver a decisive victory, and weapons have been replaced by weapons systems. For example, the patriot missile relies on multiple technologies working in concert, from satellites to the missile itself, with data being relayed around the world. Modern militaries have become reliant on electronic sophistication. The authors of *Unrestricted Warfare* assert that war has not disappeared, but its appearance has changed and its complexity has increased (Qiao and Wang 1999).

**Non-Traditional Threats**

Increasing interdependence among states has increased the danger of non-traditional security threats, including the spread of disease, environmental damage, international terrorist groups, international crime, acquisition and transportation of energy and resources, natural disasters, and intertwined economies that can have an impact on social and political issues. For example, modern transportation has made it possible for criminals to traverse the globe with relative ease. The internet allows them to transfer or hide money across the globe and to covertly communicate beyond the jurisdiction of their enemies. Natural disasters or communicable diseases are no longer something which can be kept quiet as information radiates out through global media, causing damage to soft power factors, tourism, business, and international scrutiny (China's National Defense in 2006).

The line between military and non-military, soldier and civilian, is being blurred. Terrorism is the most common example: the 2001 plane hijackings in the US, the Madrid train bombings in 2004, and the London bombings in 2005 to name just a few key examples. These lack an easily identifiable enemy to target, they cross territorial boundaries and use asymmetric attacks. Further blurring the line are the Sarin gas attacks on the Tokyo subway by disciples of the Aum Shinri Kyo, the actions of currency speculators in relation to the East Asian financial crisis, drug cartels, the mafia, media moguls who can influence the opinion of a mass audience, or industrial polluters who affect the economy and health of their



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

neighbours. These events can cause damage and disruption equal to war, but there is no foreign military or state against which to go to war. The individuals involved may be from multiple states and acting without government sponsorship.

Another form of non-traditional threat comes from hackers. Hackers tend not to have military training, they may or may not have a political agenda, and they are capable of causing massive damage with nothing more than an off-the-shelf computer and an internet connection. For example, two British teenagers were able to access files on ballistic weapons research of the US. They then took control of US air force computers and proceeded to intrude into other military and government installations, making it appear as though the US military was hacking other states (Hacking U.S. Government Computers from Overseas 2001). The rapid advancements in technology and globalization are opening new and complex ways to subvert security. In 2008, a group of 11 people managed to steal 45 million users' bank and credit card details, resulting in a loss of more than $256 million. The group members were from diverse, yet cyber-advanced, geographical locations, including: Belarus, Estonia, China, Ukraine, and the US. Their unprecedented feat was accomplished by sitting outside of TJX retail stores and hacking into the store's wireless network. This illustrates asymmetry, emerging technology security risks, globalization, and the enhanced vulnerability of commercial targets as opposed to direct military targets (Malone 2008; Almeida 2006).

**Combination**

To be militarily successful in this new era will require the ability to combine operations. Combining weapons has been used throughout military history. Horses, armour, stirrups, and swords are not as effective when used individually. Their combination can create synergy, where the combined strength is greater than the individual parts. During the Gulf War, the US combined the old A-10 ground attack aircraft with the new Apache helicopter to create a "lethal union" (Qiao and Wang 1999). By dropping leaflets and publicizing video of precision strike weaponry, the US combined PSYOPS and media warfare as well. The US has pursued additional combinations of traditional and non-traditional attack methods. During the 1979 Iran Hostage Crisis, the US initially tried traditional military force, but when this attempt failed they froze Iran's foreign assets, imposed an arms embargo, supported Iraq with weaponry and training, and began diplomatic negotiations. When all these channels were used together, the crisis finally came to an end. The Americans have also employed non-traditional attacks against non-traditional enemies. For example, they used hacking methods to search for and cut off the bank accounts of Osama Bin Laden in various states (Musharbash 2008; Vallence 2008).

China has demonstrated its commitment to such combinations. It seeks to develop military modernization and economic growth in tandem, with an emphasis on science and technology. China's 2006 defence white paper puts forth a goal to "work for close coordination between military struggle and political, economic, diplomatic, cultural and legal endeavours", using "strategies and tactics in a comprehensive way. . ." Also noted is the importance of taking part in international organizations, such as ASEAN+Three, the Shanghai Cooperation Organization, WTO, IMF, and the International Olympic Committee. These open up diplomacy, aid in soft power, and give China a voice in determining the legal framework of a globalized world (Ikenberry 2008; China's National Defense in 2006).

To learn how to conduct cyber security, the Chinese must have a full understanding of how attacks are conducted; therefore they will learn offence along with the defence - the two are

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

inseparable. China has repeatedly stated its goal of military modernization, and cyber warfare is where modern militaries are headed. However, cyber warfare would unlikely be used alone. It could be used simultaneously with a traditional attack, perhaps as a first blow to take an opponent off guard, or in tandem with multiple non-traditional attacks, such as PSYOPS and economic operations, or variants of each. Additional combined tactics that will be discussed in the following sections include cyber attack, cyber reconnaissance, and market dominance.

**Internal Security**

As seen with the lack of division between the PLA and PAP, the Chinese defence white paper's stated goal of developing the military and economy in tandem, and with the blurring of lines in Unrestricted Warfare, China cannot ignore the full spectrum of impact that Information Communication Technologies (ICT) will have, including that within its borders. China's internet population has risen to 210 million people (Anick 2008; Bridis 2008). And, as of 2007, China possessed over 500 million mobile phones. China has become a world leader in the communications industry, and 3G and 4G technology are increasing the ability for mobile phones to supplant a personal computer for online activities. On the one hand ICT supports economic, scientific, and technology development; on the other it creates a non-traditional security threat.

Social networking services can be used as a tool to further nationalistic goals. These goals may include the spread of political ideology, propaganda, and disinformation. As seen with the US Information Operations Roadmap, PSYOPS are an integral component of cyber warfare. Operatives can sway audiences by presenting well thought out arguments or by altering opposing views; they may also manipulate democratized news by artificially inflating votes using scripts (Cuban 2008). Recent informationization military courses offered at Wuhan University include "An introduction to US and Taiwanese social information systems" suggesting that China has already recognized the benefits of utilizing social networking externally (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008).

Additionally, online users are increasingly volunteering to enter large amounts of personal data, which can, and has been, used for prosecutions (Use of Social Network Websites in Investigations 2008; WFTV 2008; Layer 8 2007). Users do so to enjoy the social service it provides, either not realizing, or unconcerned, that the government is simultaneously gaining access to a self-imposed Big Brother. Not only can China use this information to its benefit, but also it must secure it from being used by an adversary, such as its use for identifying potential espionage and subversive assets. In terms of stemming anti-government agendas, state agencies censor blogs, bulletin boards, email, and forums. Internet Service Providers (ISPs) often take it upon themselves to censor users, because they are held legally responsible for any customer who violates the law. Internet cafés are required to keep detailed records of their customers. In addition, "every Chinese person who signs up for internet service must register with his or her local police department within 30 days" (China and Internet Censorship 2006).

As China's economy continues to grow, personal electronic devices are becoming more accessible to Chinese citizens. Products such as personal computers, high speed internet connections, mp3 players, large hard drives for storage, gaming systems, and advanced mobile phones fuel a desire for more software and entertainment. This will enhance



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

international criticism of Chinese copyright infringements *and* it will make it difficult for China to prevent the spread of Western culture (French 2006; People's Daily Online 2006; Pirates of the Orient 2006). Increased connectivity also increases the capability of people to conduct subversive activities that endanger state security. This may include, "Signing online petitions, calling for reform and an end to corruption, planning to set up a pro-democracy party, publishing rumours about SARS, communicating with groups abroad, opposing the persecution of the Falun Gong and calling for a review of the 1989 crackdown on the democracy protests . . ." (Kumar 2006). Other emerging non-traditional threats include mob mentality, consumer price manipulation, domestic hacker groups who can damage and interfere with the Chinese government or drag it into conflict with other states, and the security of the identity and financial details of a growing online consumer market (Delio 2001).

In addition to China's economy being directly linked to military issues, so too are domestic threats, soft power, and the control of information. Readily available free web sources, such as blogs, photo uploading, video uploading, Podcasts, torrents, and RSS feeds, have given powers to individuals that were once restricted to large media outlets. Social networking sites allow for the spread of this information across the globe at speeds exceeding traditional mass media, and they are capable of reaching larger markets. These social networking services, often referred to as Web 2.0, are noted for their ability for people to collaborate and share information online, particularly emphasizing real-time dynamic displays, interconnectedness, and being a part of a larger community. China maintains strict government control over television, newspapers, and radio; therefore these new forms of distribution pose a threat to China's control. Censorship of the internet by China, known as the Great Firewall, can be seen in the banning of foreign sites, such as Blogger and Voice of America, as well as a wide range of search terms and images the government deems a threat to national security or counter-productive to the political party. During the 2007 uprising in Tibet, China blocked access to the video website YouTube (Richards 2008), and on multiple occasions it has been accused of using Photoshop to digitally alter photos in its favour (Pasternack 2008; Yue 2008). With the increasing popularity and economic success of Web 2.0, coupled with China's global presence (prestige and international scrutiny) it is unlikely that the Chinese government will ban these new forms of news distribution on a permanent basis. However, it will seek to understand and entrench itself within the emerging system.

China has struggled to cope with internal and external cyber dissidents. This includes pro-democracy movements and the dissemination of sensitive information such as the spread of SARS and human rights abuses. Pro-democracy activists Li Yibing and Jiang Lijun of Hong Kong used virtual dead drops to secretly pass messages, such as a plot to "disrupt the 16th Communist Party Congress by phoning the police with a false bomb alert" (Reporters Without Borders 2006). Each member knew the user name and password to a single email account. They would save messages as drafts, allowing the other member to log in and read it at a later point. This avoided detection, because no message was ever sent. This represents an asymmetric advantage provided by new technology; however China demonstrated its prowess in using the same technology to combat the cyber-dissidents by using international cooperation, internet laws, and online eavesdropping. Activists can use the internet to build coalitions, create e-petitions, and organize protests, using elements such as maps, lookouts, and live broadcasts. Foreign bloggers using commercially available satellite imagery have compromised Chinese military secrets on numerous occasions. These non-governmental bloggers have uncovered a Chinese site used for developing submarine technology, a training facility used to prepare for a potential conflict with India, and the construction of a fourth

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

satellite and missile launch facility in Hainan (Reporters Without Borders 2006; Yahoo implicated in third cyberdissident trial 2006).

Determined Chinese internet users are finding ways around The Great Firewall. One popular way is to use proxy relays. A proxy server acts as an intermediate; it allows them to access banned sites through servers that are based abroad. Other techniques include using specifically designed software, circumventors, tunnelling, encryption, and cached pages. Several foreign organizations have voluntarily taken on the task of circumventing China's censorship and making this information public. Among the groups that may have breached The Great Firewall are the University of Cambridge, the University of Toronto, M.I.T., underground hackers (presumably doing it just for the challenge), and groups formed by Chinese defectors. Software such as Dynapass, Ultrasurf, Freegate and Garden Networks are used by approximately 100,000 people in China to gain access to news and information that is blocked by the firewall. With the increasing interconnectivity of modern times, China must actively defend against these internal threats or risk having collateral damage to the military, soft power, economy, and political integrity (China Tightens Vice on Internet 2006).

Despite some drawbacks, it is in China's best interest to promote the growth of the internet as it will boost the economy, improve education, and keep the nation competitive in the 21st century. New freedoms for expressing political opinion will be counterbalanced by new means of censorship and means to reduce a widening digital and social divide. The Chinese government must be moderate in its approach to censorship and the digital divide or it runs the risk of widespread dissent resulting from increasing socio-economic/rural-urban disparities. The impact of the internet on China's near future will be one of expanded growth, a complex interaction of balances, and a constant adaptation to evolving technologies from within pre-established ideologies. The following sections will further demonstrate how the average internet user is becoming intertwined with military activity.

## 3. Cyber Reconnaissance and Attack

NCW, IO, FCS, and Informationization are not identical to cyber attack and cyber reconnaissance; however they significantly overlap. The first four, discussed above, tend to deal with the hi-tech advancement of traditional military assets, PSYOPS, and media warfare – all of which rely on the internet in some form. The lexicon is continuing to develop, having at times included the terms: total dimensional warfare, expeditionary forces, command and control warfare, information warfare, full spectrum dominance, and electronic warfare. Cyber attack may be thought of as hacking with the intent to destroy or disrupt. This could include the physical destruction of a computer, deleting/re-writing of files, or knocking a network or service offline. Cyber reconnaissance is the collection of data, also known as cyber espionage or network intrusion. This may include technology transfer or intelligence, such as troop locations or weaknesses that could be used in an attack. In many cases a hacker goes from reconnaissance to attack at will. Here all six will be addressed – NCW, IO, FCS, Informationization, Cyber Attack, and Cyber Reconnaissance - as components of cyber warfare (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008).

This section will examine cyber reconnaissance with an emphasis on Chinese examples and military applications. In addition to China's stated goal of informationization and the quasi-officially endorsed book, *Unrestricted Warfare*, this section will show that foreign allegations



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

and widespread network intrusions suggest China is developing a cyber warfare capability. Cyber warfare fits with China's established patterns of asymmetry and technology transfer. In order to grasp why Beijing would pursue cyber warfare as a means of leapfrogging, it is essential to acknowledge the skills of hacking. Hackers utilize a wide range of tools with highly sophisticated techniques, the scope of which is beyond this article; however some basic understanding is necessary. Hacking is capable of causing massive damage with little funding, it is difficult to detect and defend against, it provides a high level of deniability, and it eliminates the problem of geographical distance.

**Security Hacking**

A common method used in cyber reconnaissance and attack is the security exploit. A security exploit is a prepared application that takes advantage of a known weakness. It is a piece of software, data, or commands that utilize a bug, glitch, or vulnerability to cause an unintended or unanticipated behaviour to occur on computer software, hardware, or electronic devices. This can allow the attacker to take control of the computer, permitting its use for other tactics, such as DDoS discussed below. An exploit may be used to gain low-level entrance to a computer, after which a hacker can search for further exploits to attain high-level access such as system administrator (root). This tactic is known as privilege escalation. Once exploit vulnerability has been identified by security experts, a patch will be issued. For this reason hackers try to keep known exploits secret. These are known as zero day exploits, and hackers may catalogue large numbers of them for their own use or to be sold on the black market (Hines 2008). In 2006, Taiwan was hit with "13 PLA zero-day attacks", for which it took Microsoft 178 days to develop patches (Tkacik 2007).

Vulnerability scanners may be used to identify exploits. One such scanner known as a port scanner automates the process of finding weaknesses of computers on a network. These check to see which ports on a specified computer are 'open', available to access, and sometimes will detect what program or service is listening on that port. Turning from reconnaissance to attack, once an open port is found, large quantities of data can be sent in an attempt to cause a buffer overflow. This can cause exposure of data, memory loss, and/or a crash within the compromised system.

The primary means to identify computers used in cyber warfare is the IP address. An IP address is a numerical identification that network management assigns to devices participating in a computer network utilizing the Internet Protocol (TCP/IP) for communication between nodes. In essence, each computer has its own unique IP address. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for global IP address allocation. ICANN, a non-profit organisation operating in the US, is under contract with US Department of Commerce and previously with US Department of Defense. Despite this identification tool, hackers can mask their identity by using proxy servers. Information is routed through multiple computers, only showing each computer's identity to the next in line. For example, a Chinese hacker could route his or her activity through a computer in Brazil, which routes its activity through Russia. The computer in Russia could be used to attack a computer in the US, and the US would see it as an attack from Russia. Perhaps through painstaking effort the American investigators can identify that the Russian computer was a proxy, but then they are led to Brazil. If they manage to go from Brazil to China, they are still unsure whether China was the originator or simply another link in the chain. Proxy servers can be rented or obtained through compromised systems. Additionally,

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

free software such as Tor (The Onion Router), encryption, tunnelling protocol, and wireless access points (hotspots) add additional anonymity.

A spoofing attack is when a person or program fools another into thinking it is someone or something else. One example is the man-in-the-middle attack, in which person C gets person A to believe they are person B, and they get person B to believe they are person A, thus gaining access to information sent in both directions. This is accomplished by monitoring packets sent from A to B (often involving a packet sniffer), guessing their sequence and number, knocking them out with a SYN attack, and injecting packets from C. Firewalls may defend against these attacks, if they have been configured to only accept IP addresses from the intended correspondent.

Webpage spoofing, known as phishing, imitates a webpage such as a bank's website. When the user enters their data, such as passwords and usernames, the fake website catalogues their information. Webpage spoofing is often used in conjunction with URL spoofing, using an exploit to display a false URL, and DNS cache poisoning to direct the user away from their intended site and then back again when the data has been collected. As a precaution some websites require a user to arrive at their login page from a specified referrer page, but these referrer pages may also be spoofed. During the 2008 Olympics net users in China received a high volume of email spam offering video highlights of the games. Clicking on the links brought users to spoofed CNN pages which asked them to download a codec to watch the videos; once installed the computer was compromised and become a part of the Rustock botnet, i.e. an automated 'robot' running on the web to generate false headlines that entice people to load harmful code (Miller 2008; Hi-tech Thieves Target Olympics 2008).

Spoofing may also be used defensively. For example, the Recording Industry Association of America (RIAA) has practised spoofing on peer to peer networks. The RIAA floods these communities with fake files of sought-after material. This deters down loaders by means of fear and by wasting their time and bandwidth. This could be employed in the same manner by militaries, or as a source of disinformation. A similar defensive tactic, known as a honey pot, lures criminals in by offering sought-after data or what appears to be a compromised network. The honey pot is designed to collect data on the intruder, while giving away nothing, or giving away something that is perceived as an acceptable loss to gain something greater in return.

Attackers may also compromise a computer or network by using a Trojan horse, often known simply as a Trojan. A Trojan appears to perform a desirable function, while secretly performing malicious functions. Trojans can be used to gain remote access, destroy data, download data, serve as a proxy, falsify records, or shut down the target computer at will. The Pentagon, defence-related think tanks, and defence-related contractors were the target of a combined spoofing and Trojan attack in 2008. Trojans were hidden in email attachments designed to look as if they were sent from a reliable source. The Trojan was designed to bury itself into the system, covertly gather data, and send it to an internet address in China. Due to the ability of hackers to route their activity through foreign computers, security experts were unable to determine if China was the final destination, if it was an attempt at framing China, or if it was a state-sponsored activity (Waterman 2008).

This was not the first time US research facilities received spoofed emails with Trojans purportedly from China. In 2005 the Oak Ridge National Laboratory and Los Alamos National Laboratory became infected. No classified information was believed to have been



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

obtained; however personal information of visitors from the years 1990 to 2004 was compromised. This included names, date of birth, and social security numbers. These two research facilities were originally constructed for sensitive nuclear weapons research during WWII. Today they are used 'for research in numerous areas including national security, nanotechnology, advanced materials, and energy' (Lasker 2005). In general, Cyber reconnaissance may be an attempt to attain victory conditions before battle. These intrusions, if undetected, allow intruders to identify vulnerabilities for future cyber attack. The cost of probing computer networks is low, given the lack of attribution, requiring as few as one hacker, and the ability to work from remote locations using off-the-shelf hardware.

A rootkit is a toolkit hidden on a compromised computer. The rootkit can be a diverse set of programs, but invariably is designed to hide the fact that the computer has been compromised and defending itself once detected. These rootkits often hide themselves as seemingly innocuous drivers or kernel modules, depending on the details of the operating system and its mechanisms. In addition to covering the tracks of an intruder, they can allow easier access in the future by opening backdoors. They may also include an arsenal of sniffers, key loggers, and tools that relay email chat conversations. Rootkits may also serve as a staging ground for email spam distribution and DDoS attacks as a part of a larger botnet. In 2005, it was revealed that Sony BMG included rootkit software on their CDs. This software altered the Windows OS to allow access to the computer by anyone aware of the rootkits existence, presumably to enforce copyright protection. This example shows that corporations, too, can be a part of cyber attack or reconnaissance, furthering China's desire to create its own software and establish market dominance as opposed to being subjected to the US's. Numerous source codes for ready-made rootkits can be found on the internet. In 2006, alleged Chinese hackers infiltrated "the Department of Commerce's Bureau of Industry and Security, which manages export licensing of military-use products and information" using rootkits to allow privilege escalation. The agency spent millions of dollars on new, clean, hardware and software, because they could not restore the integrity of the compromised network (Tkacik 2007).

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. The original virus may modify the copies, known as a metamorphic virus, making its destruction more difficult (similar to genetic diversity). A virus can spread from one computer to another through the internet, email, the network file system, or removable medium such as a USB drive. Damage caused by viruses include deleting files, damaging programs, reformatting the hard drive, and disrupting or debilitating the system completely. Viruses may also be used as PSYOPs or demoralizers by presenting text, video, or audio messages to the computer user. In order to replicate, a virus must be allowed to execute code and write to memory. For this reason, many viruses attach themselves to executable files, such as Word and pdf documents, or html links. Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them. The Panda Burning Incense Virus is an example of cyber warfare posing an internal security threat to China, and it set a legal precedent for pursuing and prosecuting hackers (Lemon 2007).

Like a virus, a worm is also a self-replicating program. A worm is a program or suite of programs that attempts to scan a network for vulnerable systems and automatically exploit those vulnerabilities. Some worms work passively, sniffing for usernames and passwords and using those to compromise accounts, installing copies of themselves into each such account, and typically relaying the compromised account information back to the intruder through a

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

covert channel. Many worms have been designed only to spread, and do not attempt to alter the systems through which they pass. However, the Morris worm and Mydoom showed that network traffic and other unintended effects can cause major disruption. A 'payload' is code designed to do more than spread the worm - it might delete files on a host system, encrypt files for extortion, send documents via email, or destroy the target computer by rendering it unusable.

The Code Red and Code Red II worms were the most successful worms in internet history, causing nearly $2 billion in damages and infecting over 600,000 computers. The worms, which may have originated from a university in Guangdong, China (United States General Accounting Office 2001), attacked computers running Microsoft's IIS web server and exploited a buffer overflow. Home computers were largely unaffected; however any attempt at infection caused them to crash. The worms created slow downs in internet speed, knocked websites and networks offline, and defaced websites with the phrase "Hacked by Chinese!" - although Chinese involvement was never confirmed. The attacks may have been state-sponsored, they may have been underground hackers and script kiddies, or they may have been a combination of the two. A script kiddie is not an expert in computer security. They use pre-packaged automated tools written by others and found online, such as WinNuke applications, Back Orifice, NetBus, Sub7, Metasploit, and ProRat. Even though script kiddies lack sophistication, and they are looked down on by the hacker culture, they still pose a significant security risk. When media attention is drawn to internet incidents, it is often followed by individuals seeking to participate without any coordinated effort or instructions to do so. Code Red II had a slightly different payload that could open a backdoor, leaving the computers vulnerable to further exploitation (Schwartz 2007; Cost of 'Code Red' Rising 2001).

The Code Red worms coincided with the collision of a US reconnaissance plane and a Chinese fighter jet, in which the Chinese pilot died, and known as the Hainan or EP-3 Incident. Patriotic Chinese hackers defaced dozens of US military and computer industry websites. Patriotic US hackers responded with inflammatory web page defacements, comment spamming, posting of photoshopped derogatory pictures, and probably were the source of the Code Blue Worm (Delio 2001). Code Blue sought out systems infected by Code Red and reprogrammed them to launch attacks against targets based in mainland China. In particular, it launched DDoS attacks against the Chinese security firm NS Focus. These type of attacks could be used clandestinely against one's own country to spur nationalism. Or cyber attacks could be used by a third party state, or organization, to create conflict between external states to further some masked goal. For example, Iran could benefit by creating tension between the US and China through an attack prior to a US proposed UN resolution, in which China has veto power (Onley and Wait 2006; Delio 2001).

In 2004, the Myfip worm probably originated from IP addresses in the Chinese municipality of Tianjin (Brenner 2005). This worm stole pdf files, with later variants targeting Microsoft Word documents, schematics, and circuit board layouts. Among the victims were Bank of America, BJ's Wholesale Club, and Lexis-Nexis. The worm not only stole intellectual property, such as product designs, but also took customer lists and databases. Identifying the number of companies affected poses difficulties as they do not wish to further damage their business by coming forward. To do so can damage consumer confidence and require the



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

implementation of costly security measures. Businesses may also be oblivious to the number of previous infections and potential data loss as they simply update their patches and move on (Brenner 2005).

A denial-of-service (DoS) attack or distributed denial-of-service (DDoS) attack is an attempt to make a computer resource unavailable to its intended users. This is accomplished by flooding the target with data requests, so that it cannot respond to legitimate traffic, or so that it responds so slowly that it is rendered useless. DDoS attacks may be conducted by a collective of individuals, often co-ordinating their efforts, or by a network of computers under the control of a single attacker. Such networks are called botnets, with each computer in the botnet being known as a bot, or a zombie. These computers have been taken control of by malicious users without the knowledge of the owner, usually through a rootkit, Trojan, or virus. Sobig and Mydoom are examples of worms which created zombies. A botnet's originator, known as a bot herder, can control the group remotely, usually through a means such as IRC, and usually for nefarious purposes. Infected zombie computers are used to send email spam, to host contraband data such as child pornography, or to engage in distributed denial-of-service attacks as a form of extortion. The services of a bot herder can be rented on the black market. One estimate suggested that Chinese hackers have 750,000 zombie computers in the US alone (Waterman 2007). A similar, but non-malicious, phenomenon involving the banding together of excess computer power can be seen in the Search for Extra-Terrestrial Intelligence (SETI@home), or Stanford University's protein folding simulations (Folding@home).

DoS and DDoS attacks can prevent an internet site or service from functioning temporarily or indefinitely. DOS attacks can also lead to problems in the network branches around the actual computer being attacked. For example, the bandwidth of a router between the internet and a local area network may be consumed by an attack, compromising not only the intended computer, but also the entire network. If the attack is conducted on a sufficiently large scale, entire geographical regions of internet connectivity can be compromised without the attacker's knowledge or intent by incorrectly configured or flimsy network infrastructure equipment. Scripts can be set up to automate the process, and subtle variations of these attacks, such as smurf attacks, fraggle attacks, teardrop attack, ping flood, SYN flood, IRC floods, banana attack, Fork bomb, pulsing zombie, and nuke exemplify their sophistication. Various DoS-causing exploits such as buffer overflow can confuse server-running software and fill the disk space or consume all available memory or CPU time. A permanent denial-of-service (PDoS), also known loosely as phlashing, is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. Unlike the DDoS, a PDoS attack exploits security flaws in the remote management interfaces of the victim's hardware, be it routers, printers, or other networking hardware. These flaws leave the door open for an attacker to remotely 'update' the hardware firmware to a modified, corrupt or defective firmware image, therefore bricking the device and making it permanently unusable for its original purpose. The PDoS is a hardware-targeted attack which can be much faster and requires fewer resources than using a botnet in a DDoS attack.

It is important to note the difference between a DDoS and DoS attack. If an attacker mounts a smurf attack from a single host it would be classified as a DoS attack. In fact, any attack directed against computer availability would be classified as a DoS attack. On the other hand, if an attacker uses a thousand zombie systems to simultaneously launch smurf attacks against a remote host, this would be classified as a DDoS attack. Several botnets have been found and removed from the internet. Dutch police located and disbanded a 1.5 million node

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

botnet, and the Norwegian ISP Telenor disbanded a 10,000 node botnet (Keizer 2005; Leyden 2004). Large, coordinated international efforts to shut down botnets have also been initiated, such as Operation Spam Zombies, which included agencies from 25 different states (Operation Spam Zombies 2005). It has been estimated that up to one quarter of all personal computers connected to the internet may become part of a botnet. And an estimated 50% of all pirated Windows programs contain pre-installed Trojans. China is renowned for its use of pirated Windows programs. This is a cause for concern for China as it bogs down internet and computer efficiency. It also could make Chinese computers susceptible to international condemnation, if their computers are used via proxy. Further, it demonstrates to China the value of developing its own operating systems for domestic and world markets, either to avoid such problems, or to create them for others (Weber 2007).

There are also hybrids. A worm can install a rootkit, and a rootkit might include copies of one or more worms, packet sniffers, or port scanners. A rootkit or virus may be used to conduct a DoS attack, and compromising the system may include some traditional social engineering (HUMINT). So all of these terms have somewhat overlapping usage and they are often misused by mainstream media. The depth of security hacking goes far beyond the examples given here. These examples serve as an introduction to the level of sophistication with which computers can be compromised, illustrating the difficulty in providing defence. They also demonstrate the high level of damage that can be caused by a small group of individuals who work with little funding. This adds to the lack of attribution as it does not require the funding and support of a military, making state-sponsored hacking easy to deny. In combination with anonymity tools and the ability to hide intrusions, security hacking provides a high level of stealth and asymmetry.

**Military Applications of Hacking**

The USA's paramount position and its heavy reliance on computers have made it a prime target. For this reason it has some of the most extensive information on cyber attacks. The United States has had millions of computers infected at a cost in the billions of dollars. Hackers may be lone teenagers searching for fun or curiosity or state-sponsored intelligence gathering and technology transfer, the determination of which is highly problematic. Frequently hit targets include the US Department of Defense, the Pentagon, NASA, Los Alamos Laboratories, Boeing, Lockheed Martin, Northrop Grumman, Raytheon, Harvard University, California Institute of Technology, and a wide range of think tanks, defence contractors, military installations, and high profile commercial corporations. The attacks have come from across the globe and identifying and prosecting those responsible has proven difficult (Greenberg 2007; Hacking U.S. Government Computers from Overseas 2001).

These hackers have been able to steal classified data, such as naval codes, information on missile guidance systems, personnel performance reports, weapons development, and descriptions of the movement of equipment and personnel. Jonathan ("c0mrade") James downloaded $1.7 million worth of software used to control the International Space Station's life support. Dutch teenagers stole information on the Patriot rocket launching system, and the Navy's Tomahawk cruise missile, and tried to sell it to Iraqi officials during the Gulf War – Iraq thought it was a hoax and declined (Miklaszewski 1999). Hackers have commandeered US commercial, educational, and military computers and used them in attacks against other nations, including Taiwan. Hackers can cause an immense amount of damage to a state, stealing information, deleting and changing files, transferring capital, and



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

destroying programs or entire networks (Hacking U.S. Government Computers from Overseas 2001; Christensen 1999; Qian and Wang 1999).

In 2001 and 2002 Gary ("Solo") McKinnon probed US Army, Navy, Air Force, Department of Defence, and NASA computers causing $700,000 worth of damage, taking down a network of 2,000 computers, accessing classified data, deleting and re-writing files. He accomplished this on his own from his home in London using commercially available software and a dial up connection. McKinnon claims he was searching for proof that the US is hiding information about UFOs and an anti-gravity propulsion system. This illustrates the relative ease with which intrusions can take place, the difficulty of determining whether or not it is a state-sponsored action, and a lack of legal framework for timely response. With such attacks occurring so frequently to vital industries, the US, with the largest military budget in the world, has inevitably developed a means to defend against them, which by association means they have also developed the means to conduct cyber reconnaissance and cyber attacks itself. China, too, is the subject of frequent attacks, albeit less publicized, and it will want to remain competitive with US military capabilities (Boyd 2008; Bruno 2008).

**Titan Rain**

A coordinated series of attacks against US installations are strong indicators that China is developing a cyber warfare capability. The attacks which ran from 2003 to 2006 were designated 'Titan Rain'. They targeted US defence and aerospace installations, Sandia National Laboratories, Lockheed Martin, Redstone Arsenal, the Department of Defense, and NASA, gathering sensitive military data. The United Kingdom also reported being attacked by the Titan Rain hackers. Much of the data stolen was not classified; however it was not meant for public or foreign consumption, nor was it meant for unlicensed use. For example, the US military's classified data is typically not connected to the broader internet, but sensitive information such as logistics support for the armed forces is. This can provide valuable insight into field tested experience, as well as expose possible weaknesses to an adversary (Brenner 2007; Espiner 2005).

In addition to the unauthorized gathering, the US is concerned that enough of this data could be used to piece together a larger picture, one that would be considered classified. Among the information gathered were "a stockpile of aerospace documents with hundreds of detailed schematics about propulsion systems, solar panelling and fuel tanks for the Mars Reconnaissance Orbiter . . . specs for the aviation-mission-planning system for Army helicopters, as well as Falconview 3.2, the flight-planning software used by the Army and Air Force" (Thornburgh 2005). Although the majority of data appears to have been benign, its massive quantity may one day prove to include items that the US deems classified at a later date. These attacks could be a staging ground, testing US defences, for future operations of a more serious nature.

Titan Rain demonstrated how China could use cyber warfare as an asymmetric tactic (Norton Taylor 2007). Apparently, a team of hackers, estimated to number between 6 to 30, would take control of US defence computers, copy everything on the hard drive within 30 minutes, and send that data to zombie computers in South Korea, Hong Kong, or Taiwan, where it was subsequently routed to computers in the Chinese province of Guangdong. The ability to route the data makes it difficult to prove the attacker's identity. While it is believed China was responsible, there is no certainty that the data was not further routed to another location. Additionally, those computers may have been under remote control by a separate

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

government, or the hackers may not have been state-sponsored. The attacks themselves were not particularly sophisticated, requiring only minimal training with commercially available products. The instructions on how to conduct such attacks are widely available on the internet itself (Delio 2001). But attempts to identify the attackers would require the burdensome task of sending covert agents to physically identify the source.

By using the virtual world, hackers are able to traverse great distances without leaving their station. On the night of November 1, 2004, Titan Rain members scanned, broke into, and retrieved data from defence installations in Arizona, Virginia, California, and Alabama (in that order) all within a period of six hours. Once attackers gain control of US computers, through methods such as Trojans, they can not only shut down the system, they can also conduct attacks using those computers. This could be used to raise condemnation of the US, as it would appear the US is attacking other states (Graham 2005; Thornburgh 2005). While proof is non-existent, some US officials believe that the PLA was responsible (Norton-Taylor 2007). Chinese military doctrine repeatedly discusses "the importance of penetrating an adversary's military logistics and personnel networks. Furthermore, the multiple intrusions into what nuisance and criminal hackers would regard as boring, mundane networks--networks that do not offer the treasure trove of credit card numbers, bank accounts, and identity data that criminal hackers typically seek-- suggest a military purpose" (Tkacik 2007).

**Further Evidence of Build-up**

Attacks under the code name Titan Rain have ceased. However, OSINT suggests that cyber attacks from China persist. From 2005 to 2007, the US State Department, Bureau of Industry and Security, DoD, National Nuclear Security Administration, Department of Homeland Security, Boeing, Northrop Grumman, Raytheon, Lockheed Martin, and defence-related think tanks had intrusions from Chinese ISPs (China's Proliferation Practices and the Development of Its Cyber and Space Warfare Capabilities 2008; Leyden 2007, Tkacik 2007, Almeida 2006). Sensitive but non-classified data continues to be harvested; items such as emails and the 'names and other personal information on more than 1,500 employees' (Onley and Wait 2006). Attacks from Chinese ISPs have forced entire networks to be taken offline or replaced. In 2005 alone, 'the Pentagon logged more than 79,000 attempted intrusions' (Reid 2007). Cyber reconnaissance and attacks from Chinese IP addresses had become so frequent and aggressive that US President George W. Bush raised the subject to Chinese President Hu Jintao at the APEC summit in 2007.

The difficulty of attribution in cyber attacks, such as proxies, botnets, non-state-sponsored hackers, and a lack of legal framework to pursue them, means these attacks may not have come from China; however the accusations alone are evidence that China will want to develop a cyber warfare capability. China now has the world's largest internet population, so in terms of volume, China has the most targets to defend. Chinese officials have stated that they are the victim of 'massive and shocking losses of state and military secrets via the Internet' (Leyden 2007). Foreign states wishing to use cyber warfare against the US may recognise the focus being placed on China and use Chinese computers to conduct their own reconnaissance and attacks by using botnets or proxies based there. Further, denouncements by the US may indicate that retaliatory responses are in the works and that the US will use allegations of Chinese incursions to bolster support for increasing US cyber warfare capability, thereby putting China further behind in military competitiveness. Damage to China's soft power, particular in relation to ICT, may affect China's economy by making investors cautious and export controls/legal bureaucracy more stringent. PSYOPS campaigns



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

and media warfare, of the type outlined by the US Information Operations Roadmap (discussed above), may help China regain its lost credibility. These are elements of cyber warfare, but viewed as less offensive than reconnaissance and direct cyber3 attack.

**Non-US Foreign Allegations**

The US is not alone in accusing China of using cyber warfare. In 2007 and 2008, China was publicly accused of hacking into government facilities by officials in Australia, France, Germany, India, Japan, New Zealand, South Korea, and the UK (Basu 2008; Goodin 2008; Ha 2008; Leyden 2007; Marquand 2007). The number of countries under Chinese attack could be far greater as some may not know that they are under attack, may not wish to reveal their weakness due to a loss of soft power and consumer confidence, or they do not wish to upset China as a valuable trading partner. Hans Elmar Remberg, Vice President of the German Office for the Protection of the Constitution (Germany's domestic intelligence agency) stated that "across the world the PRC is intensively gathering political, military, corporate-strategic and scientific information in order to bridge their technological gaps as quickly as possible" (Tkacik 2007).

Unlike HUMINT, cyber warfare provides a lack of definitive attribution, makes distance nearly irrelevant, allows for the mass accumulation of data in a short span of time, and at a small cost in comparison to traditional espionage or military activities. Cyber attacks, such as an incident that shut down the UK House of Commons, may only be small scale test runs, probing, or reconnaissance blunders, meaning that the true scope of cyber attack has yet to be seen (Norton-Taylor 2007). Cyber reconnaissance appears to be the most beneficial tool of cyber warfare. Beyond finding exploitation points in the military for future attack, the commercial sector allows China the opportunity to skip generations of research and development efforts, levelling the playing field in science and technology, and by association boosting economic and military might. Chinese hackers have even gone after British parliamentiary files on human rights issues, showing a potential interest in relation to soft power, globalization, international condemnation, and the legal apparatus. As *Unrestricted Warfare* has shown, there are no boundaries in relation to such military operations.

## 4. Case Studies: Estonia, Georgia and Chanology

The 2007 cyber attacks against Estonia, Georgia and Project Chanology are examples of large-scale cyber attacks. The Estonian attacks were the first to show how cyber attack against a state provides a debilitating effect at a low cost, a lack of attribution, a lack of legal framework in defence, world-wide attention, and may point to a new arm of traditional attack. The Russo-Georgian war of August 2008 was even more sophisticated and intense than the Estonian case, showing the maturation of the process. Project Chanology reveals how the collective masses can use online tools to emerge as a powerful force without a central leadership. This can be harnessed by military power through the tactics described in IO (Information Operations, see above). And as a matter of internal security, Chanology-style movements must be carefully observed as they pose a non-traditional threat. Estonia and Chanology are an emerging expression of warfare that is fuelled by new powers afforded by the internet, but spills over into the real world, not only through financial loss and media coverage (soft power), but also in the form of volatile protests, disruption, mob mentality, and the capability of drawing governments and militaries into unwanted actions.

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

## Estonia

In 2007, the Estonian government relocated a Soviet-era war memorial and bronze statue in Tallinn, stating that the memorial symbolised Soviet occupation. The Russian government condemned the relocation, claiming it was a tribute to those who fought in World War II. The relocation sparked protests which resulted in 150 injuries, one death, and a month-long cyber war campaign. Estonian websites including parliament, banks, ministries, schools, and newspaper outlets were attacked with DDoS attacks and web page defacements. Some websites also redirected users to images of Soviet soldiers and quotations from Martin Luther King about resisting evil. Hackers who hit the ruling Reform Party's website left a fake message that the Estonian prime minister and his government were asking for Russian forgiveness and promising to return the statue to its original site (The Cyber Raiders Hitting Estonia 2007).

These attacks garnered world-wide attention. The Russian government was directly accused by media outlets and the Estonian Prime Minister Andrus Ansip. Russia had the motive and the means for such an attack. However, there was no direct evidence to suggest that the attacks were state-sponsored. There was evidence that some of the IP addresses used in the attacks belonged to Russian government officials, and instructions on how to carry out cyber warfare did circulate on Russian websites. However, the source of DDoS attacks could have been masked by using proxies or botnets that are located across the globe. Neither NATO nor European Commission experts were able to find any proof of official Russian government participation. Further, the Russian government denounced Estonia's claims and refused to participate in any type of investigation (Bright 2007; Estonia Fines Man for 'Cyber War' 2008; Estonia Hit by Moscow Cyber War 2007).

## Debilitating Effect at a Low Cost

The effects of the cyber attacks were magnified as Estonia is one of the most internet-savvy states in the European Union (The Cyber Raiders Hitting Estonia 2007). The Estonian government has pursued a paperless society, or e-government, and web-based banking. Slowing down, or halting, banking services and newspaper outlets that rely on advertising revenue strains the economy. This happens not only through a direct loss in revenue, but also with a reduction in productivity, lost efficiency, diverting resources, escalating frustration, and lost consumer and investor confidence. Estonia also uses the internet to elect parliamentary officials, file their taxes and, via mobile phone, shop or pay for parking. In some cases, website administrators simply blocked access from foreign states. While this was effective in curbing the attacks, it completely cut off banking services to Estonians outside of the country, vital to Estonian business people abroad. Spam emails inundated government officials' inboxes, halting online communication from the Parliament's email server. Officials closed off large portions of their network to keep more vital areas online. A government briefing site was given high priority while the president's website was sacrificed. The 10 largest swarms of data requests by the hackers absorbed 90 megabits per second for up to 10 hours each, straining Estonia's networks. It was 'equivalent to downloading the entire Windows XP operating system every six seconds for 10 hours' (Landler and Markoff 2007). The cyber attacks on Estonia came close to shutting down the country's digital infrastructure. While these may seem more of a disruption than a collapse, the effects radiate out into society (Bright 2007; Estonia Hit by Moscow Cyber War 2007).



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

The month-long campaign caused companies to put resources into alternative infrastructure, such as going back to traditional mail, relying on telephones, fax, and libraries, and re-enforcing alternative methods of payment. As well as the cost of material infrastructure, these type of cyber attacks cause a loss in productivity. This includes paying more people to staff bank tellers, increased traffic on the streets, and long lines at retail outlets. Newspaper outlets, telephone companies, and product distributors, have grown accustomed to using online tools, and now rely heavily on them. While this might be a boon for some industries, the whole restructuring process weakens the nation in the short term. The cyber attacks are comparable to the damage caused to industry (beyond tangible infrastructure) by flooding or blizzards. It places a nation in a state of flux, and leaves it more vulnerable to a traditional attack.

DDoS attacks offer an enemy country an effective low cost assault with high deniability. The majority of attacks on Estonia were DDoS, clogging its servers, switches, and routers. Analysis from Arbor Networks revealed thousands of bots were used against Estonia from locations as diverse as the US, Vietnam, Peru, and China. The cost to a state wanting to establish botnets is minimal, requiring only one person, an internet connection, and a basic computer. While the information for conducting such attacks can be found online, it is more likely someone with expertise, such as non-government hacker groups, would be involved in securing the rental of a botnet. This still keeps the number at a minimum, and hackers can find alternative ways to fund the rental of servers with high bandwidth, such as credit card theft (Waterman 2007; The Cyber Raiders Hitting Estonia 2007).

**Deniability**

Determining the source of DDoS attacks is a difficult task, as they can be conducted with proxies or botnets. Even if an IP address is obtained, there is no certainty that that was the true source of the attack and not one link in a chain of computers or simply a compromised computer being used unbeknownst to the owner. Message boards and chat rooms located on Russian websites served as a meeting place for attackers, a place to coordinate their time of attack, discuss targets, and recruit others. Because these individuals can be scattered across the globe, it is difficult to assign a group identity to them. The web host may not be aware that plans are being laid on their website, or they may not realise the scope of such plans. These discussions can appear as a childish prank, overshadowing the serious repercussions of the actions taking place, with no individual feeling responsible to put a stop to it.

The Estonia cyber attacks raised debate as to whether they were sponsored by the Russian government. Some believed the attacks were too sophisticated to be the work of individuals or even organised crime. Others believed the attacks were endorsed and guided by the Russian government, but thought they were not directly involved – using online operatives and media warfare as mentioned in IO. Russia has been accused in the past of sponsoring 'web brigades' - cyber attack teams - that conduct PSYOPS, disinformation, spamming, and cyber bullying, such as revealing an enemy's personal details (Polyanskaya 2006). From the perspective of officials from the United States Computer Emergency Readiness Team and the Pentagon's Defense Advanced Research Projects Agency, the attacks were not conducted by sophisticated means, nor were they state-sponsored. The attackers used commercially available off-the-shelf computers and scripts that are readily available on the internet (Waterman 2007). Data from the Arbor Networks Active Threat Level Analysis System (ATLAS) indicated that the attacks were conducted by multiple distributed botnets which appeared to have been acting independently (Kerner 2007). Even if the attacks were traced to

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

Russian government computers there was no certainty that those computers had not been taken over by remote hackers. It would also seem foolish for the Russian government to use its own computers for such an attack, especially when it has the expertise to mask its identity, unless doing so *was* masking its identity (knowing that you know I know). Johannes Ullrich, chief research officer of the Bethesda, stated: "Attributing a distributed denial-of-service attack like this to a government is hard. It may as well be a group of bot herders showing patriotism, kind of like what we had with Web defacements during the US-China spy-plane crisis [in 2001]" (Brenner 2007).

As evidence of the Estonia case continued to be examined, the consensus was that the Russian government was not directly involved. It appeared to have been "hacktavists" or simply a mass number of individuals upset over the relocation of the statue. Plans for the attacks were posted on internet forums, message boards, and chat groups prior to the attacks, including detailed instructions on how to send disruptive messages and which Estonian websites to use as targets. The discussion of proposed attacks had become so popular that it was indexed by Google, causing a Google search for the topic to return these incendiary websites at the top of its search results, bringing them to the attention of even more people. Despite being aware of these discussions prior to the attacks, Estonia could do little to stop them. Estonian officials could not identify the individuals discussing attacks, as online (not real) names were used, and obtaining IP addresses would involve going after the website administrator and foreign ISP – a task with which mega-corporations such as the MPAA and RIAA have difficulty, despite their massive funding and even when going after domestic IP addresses. Further, there is no certainty that an individual participating in the discussion will act on his or her comments, there were mass numbers of people involved (each with a different IP address, ISP, and host state to deal with), and there is no solid legal apparatus in place to deal with such an undertaking. Nonetheless, there was a growing and visible threat.

Estonian officials may have been better off devoting their resources to plant online operatives. These operatives could have placed well thought out comments to try and sway the crowd. Rather than spending all resources on physical prevention, some resources could be used to train operatives in PSYOPS, mob mentality, propaganda, and logical deterrents such as subtly mentioning flaws in their arguments, or the consequences of participating in such an attack. In order to be effective this would also require an in-depth understanding of internet subcultures (List of Internet Phenomena 2008; Pang 2008; Slashdot Subculture 2008; Slashdot Trolling Phenomenon 2008). Subtle techniques, such as self-deprecating humour, can sway the crowd's emotions and train of thought (Landler and Markoff 2007). Russian government involvement may have been as an instigator, knowingly or not, as "there [were] anti-Estonian sentiments, fuelled by Russian state propaganda, and the sentiments were voiced in articles, blogs, forums and the press" (The Cyber Raiders Hitting Estonia 2007). This could be a type of outsourcing of activity that provides a low cost attack with high deniability. Once in the hands of an unwitting mob, the tools necessary are readily available and the means are simple, thereby coordinating a massive data request simultaneously. On an individual level it takes very little effort, yet as a combined whole it has devastating effect with emergent sophistication. This small individual role, may also cause participants to feel less responsible (Estonia Fines Man for 'Cyber War' 2008).

## Legality

In addition to the difficulty of identifying the source of a cyber attack, a lack of legal framework to deal with such an attack makes it exceedingly problematic. Only one person



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

has been charged and convicted in connection with the Estonian attacks. Dmitri Galushkevich was fined 17,500 kroons for attacking the Reform Party website. Galushkevich admitted to his assault on the site, and he is believed to have acted alone. Several leads in identifying other potential participants in the Estonian attacks relied on Russian cooperation. Estonia made a formal investigation assistance request under a Mutual Legal Assistance Treaty (MLAT) between the states. Moscow appeared as though it would help, but after a delay in action, it ultimately refused to cooperate, stating that the proposed investigation was not covered by the MLAT. Further, the Head of the Russian Military Forecasting Centre stated that the attacks against Estonia had not violated any international agreements because no such agreements exist (Alo 2007; Sobrale 2007). A pro-Kremlin youth movement called The Commissar of the Nashi, claimed responsibility for some of the attacks – however, the group is located within Moldova and Transnistria which are beyond the jurisdiction of Interpol and no MLAT applies. This severely hampers the investigation as pursuing all-EU arrest warrants for these suspects would be largely a symbolic gesture (Commissar of Nashi 2007; Estonia Fines Man for 'Cyber War' 2008; Ministry of Internal Affairs 2007).

## International Publicity

Regardless of whether the attacks were state-sponsored, the Estonian incident brought cyber warfare to the attention of the global community. The case was studied intensively by many countries and military planners, since it was believed to have been state-sponsored and a modern example of a large-scale attack. Experts from the North Atlantic Treaty Organization (NATO), the European Commission, and organisations from the US and Israel were dispatched to offer assistance and collect first hand analysis of the event. The implications are far reaching: "For NATO, the attack may lead to a discussion of whether it needs to modify its commitment to collective defense, enshrined in Article V of the North Atlantic Treaty" (Landler and Markoff 2007). There is no precedence for an attack of this type. If a state's communications centre is attacked by a missile, it is considered an act of war. But what is the response to a cyber attack on that same installation, with the same debilitating effect? The Estonian attacks have encouraged the development of a NATO Cybernetic Defence Centre in Estonia. This is an extension of Estonia's 1996 push for the expansion of computer and network infrastructure in Estonia, nicknamed the Tiger's Leap (Bright 2007; A Cyber-Riot 2007; Estonia Has No Evidence of Kremlin Involvement 2007).

## Georgia

The 2008 war between Russia and Georgia over South Ossetia appeared to mirror the Estonian attacks, hinting that cyber warfare may become a standard addition to traditional warfare, whether that be state-sponsored or not. Hours after fighting broke out, "Russian hackers had established a site, StopGeorgia.ru, where visitors could view a list of Georgian websites being targeted, showing which sites had been successfully brought down, and download a simple program that enabled their own computer to join the attack" (Waterman 2008). The attacks included DDoS attacks from six different botnets against government and news websites, webpage defacements, spamming, the distribution of Georgian officials' email addresses, and distribution of a list of Georgian websites with known security flaws. The level of sophistication and intensity of the Georgian attacks surpassed that of the Estonian attacks, showing that capability is increasing. Russian-based hackers tried to halt the Georgian hacker community from responding, by taking down the two highest-profile Georgian hacker sites, hacker.ge and warez.ge, in their initial assault (Waterman 2008). However, Georgian hackers did respond, going after Russian news sites, and in some cases,

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

spoofing those sites to redirect traffic to pro-Georgian news sources (Coleman 2008; Griggs 2008). Georgian officials asserted that the Russian military was behind the attacks, but they could not provide concrete evidence. Regardless, it represents a new aspect to warfare that must be taken into account. Patriotic cyber attacks may now accompany all traditional wars. If this is not shaped according to government objectives, it runs the risk of undermining operations. For example, patriotic cyber attacks could damage soft power, they could incite damaging retaliatory attacks, and they could drag state powers into conflict.

**Chanology**

China may wish to tap into the power of a broader range of internet users, those who are not government sponsored, nor skilled hackers, yet have wide-ranging knowledge of the internet through frequent use. In one view:

> I've always argued that I do not believe the patriotic hackers are dedicated government agents, but I do believe that they are treated as useful idiots by the Chinese regime, and that the Chinese regime has figured out a rough method, using the propaganda apparatus, to shape the behavior of these patriotic hacker groups, many of whom are getting older and going from black hat to gray hat to white hat, and they want wives and jobs and houses, and the only way to get certified as an information security professional in China is to be certified by the ministries of public and state security. (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008)

A powerful array of tools is openly available to anyone with an internet connection, and they require little effort to learn. Free web-space, image and video uploading sites, such as blogs, Flickr and YouTube, give anyone with an internet connection multimedia sharing tools that rival traditional media. Social networking sites, such as Facebook and Digg, provide additional means to spread this information to a massive audience which, given enough popularity, draws in the traditional media as well. China can use propaganda and PSYOPs to influence this crowd, using it as a political tool. For example, it can be used to organise protest and cyber attacks denouncing Japan's lack of remorse for WWII atrocities, to criticize Falun Gong followers, or to rally support for the One China Policy (Faiola 2005). Project Chanology gives insight into how these non-hacker internet users can come together towards a common goal of disruption using the rapid growth of available internet capabilities. It also illustrates a growing need to understand these emergent communities as they pose a non-traditional security threat.

Project Chanology was a series of cyber attacks and real life protests organised over the internet against the Church of Scientology (CoS). The CoS is the largest organization devoted to the practice and promotion of the Scientology belief system. They are often criticized as being a cult which tries to exploit people for financial gain. A loose group of internet users named Anonymous orchestrated attacks against the CoS using multiple image boards, such as 4chan, 7chan, 12chan, 420chan, and 711chan, as well as supplementary wikis, IRC channels, YouTube, Facebook, Slashdot, Digg, and Encyclopaedia Dramatica. Users of the channels are collectively known as Anonymous, or anon, due to the website's use of anonymous posting; however their internet networks extend beyond the image boards. A large and diverse population of internet users identify with the name Anonymous, many having differing viewpoints and objectives. This point is often lost on the media, who mistakenly believe Anonymous represents a cohesive group. Anonymous is connected, but the nodes which connect each member are not the same, and therefore they do not all rally to the same cause.



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

Project Chanology was officially launched in the form of a video posted on YouTube on January 21, 2008. The video stated that the attacks where in response to Scientology's internet censorship, dubious recruitment tactics, saturating of disaster areas to 'help' victims, and overall belief system. Of particular contention was Scientology's forced removal of a leaked Tom Cruise video interview, in which he expounded his love for Scientology. Additional complaints against the CoS include the removal of leaked Scientology belief documents (part of a 10-year legal battle against Karin Spaink and several ISPs), and the attempted removal of the newsgroup alt.religion.scientology from Usenet, which led the hacker group Cult of the Dead Cow to declare war on the Church of Scientology as early as 1995. Anonymous's stated intent was to 'expel the church from the internet' and to 'save people from Scientology by reversing the brainwashing'. This was followed by DDoS attacks, black faxes, prank calls, false deliveries to CoS buildings, the dissemination of Church leaders personal information (telephone numbers, social security numbers, and addresses), and the publishing of the contended leaked material on a wide range of websites.

Project Chanology members grew to approximately 9,000 people. They successfully took down the Scientology website on January 18, 2008 with a mid-range DDoS attack. By comparison a botnet can launch a simultaneous attack from 50,000 computers. Nonetheless, Anonymous managed to cripple the Scientology website for a period of two weeks. In response to the attacks, the CoS moved its internet domain to a more secure provider. The original declaration of war video, which utilized a synthesized voice, was viewed over two million times within 18 days of its release. Project Chanology garnered mainstream media coverage on an international scale. Mainstream media's attention created an unintended DDoS attack by drawing more attention to the CoS website. Anonymous further raised questions about Scientology's actions, including the death of Lisa McPherson, a scientologist who died in 1995, for which the CoS was previously under federal investigation. Anonymous used a Google bomb technique to make the Scientology.org website the first result in a Google search for 'dangerous cult' (McMillan 2008; O'Connell 2008; Vamosi 2008; Cook 2008; Single 2008; Ramadge 2008; The Passion of Anonymous 2008).

Utilizing a wide range of online communication tools, and a new YouTube video titled "Call to Action", Anonymous coordinated a series of protests. In the video anon states: 'We have no leaders, no single entity directing us.' On February 10, 2008, approximately 7,000 people protested throughout 100 cities in 14 countries. Protesters wore Guy Fawkes masks from the V for Vendetta film, and made Rick Astley's pop single "Never Gonna Give You Up", a theme song for the protests against Scientology. The seemingly bizarre and childish behaviour of Anonymous is a part of their cohesion, a subculture of memes, slang, and humour. A second series of protests began on March 15, 2008, with approximately 7,000 to 8,000 protestors throughout 100 cities in 10 countries. CoS has not released an official estimate of the financial damage caused by Project Chanology. However, they have publicly stated that they were forced to increase online security, hired off-duty police officers to provide physical security at their churches, and have suffered increasing negative press and scrutiny from the US Federal Bureau of Investigation. CoS has denounced Anonymous as cyber terrorists and Anonymous has since switched its campaign to go after Scientology's tax-exempt status.

China could use online operatives to incite this type of internet based 'mob'. It could be used constructively within China, such as undermining the Falun Gong, or destructively against an enemy country, such as inciting protests against pro-democracy Taiwanese leadership.

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

Additionally, these online communities pose a security threat, and should therefore be examined if only as a means of deterrence. As mentioned in IO, this sort of emergent mob is not one that can be quickly understood. To be used as a military tool, China would need a deep understanding of the asset's culture. In the case of Anonymous, this equates to a heavy reliance on inside jokes, slang, internet and pop culture. Anonymous uses humour to unite and to obfuscate logic and responsibility. Credence within the group may come from inside jokes and creativity, rather than sound information – they even revel in their own failure. Internet communities can lack a centre of command, and be composed of serious, moderate, and casual participants, all of whom may change their level of participation on a whim.

## 5. Assassin's Mace

Assassin's Mace, or *shashoujian*, is used in Chinese military writings to describe a weapon or tactic 'which can deliver decisive blows in carefully calculated surprise moves and change the balance of power' (Johnston 2002). Similar concepts can be seen throughout China's history, from Sun Zi's (tr. 1963) *The Art of War* to Mao Zedong's (tr. 2000) *On Guerrilla Warfare*. An assassin's mace gains strength by ignoring pre-established rules of conduct. It has many similarities to asymmetric warfare, such as being a novel way to level the playing field, but it differs in that it is a decisive weapon, aimed at incapacitating an enemy, 'suddenly and totally' (Navrozov 2005). China possesses several asymmetric, highly devastating weapons, such as a limited but modernising nuclear weapons capacity, China's ASAT capability, and its electromagnetic pulse (EMP) capability. However each of these has considerable drawbacks. For example, human rights and environmental concerns have relegated nuclear weapons to the role of deterrent and introduced limited warfare. By using cyber warfare, China could achieve the same asymmetric destructive power while bypassing the drawbacks.

It is unlikely that China would use kinetic kill weaponry, such as its direct ascent ASAT, in an attempt to disrupt US space based assets. To disrupt US satellite dominance would require a massive sky clearing operation, because the US has constellations of satellites with multiple redundancy. The US GPS provides tactical communication and precision navigation, making it a desirable target – however, the GPS uses at least five space satellite constellations. When one is destroyed, others can be manoeuvred to fill holes in the net. Not all of these satellites are within striking range at any given time. This means a sky clearing operation would take a significant amount of time, thereby revealing Beijing's intentions. This would cause international dispute due to space debris, and allow the US to manoeuvre its other satellites out of harm's way. It would risk retaliation in which China would be at a disadvantage. Additionally, there is no guarantee an attempt would be successful, as each launch requires precise targeting, and China's ASAT has only been tested once. It is more likely China would attempt to knock out the corresponding relay stations on Earth by using a cyber attack. Chinese tacticians have focused on neutralising the uplinks and downlinks of the space-based systems through diverse forms of cyber attack including simple DoS attack. This gives the advantages of deniability and low cost. It would remove distance from the equation, allowing multiple targets to be taken out simultaneously regardless of location, and it would remove international condemnation and/or involvement (Waterman 2008; Tellis 2007; International Assessment and Strategy Center 2005).

China could destroy a vast majority of US electronics, including computers, cars, phones, and the power grid, using EMP weaponry. This is something of which all nuclear armed states



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

are capable by means of high altitude nuclear explosions, taking as few as three to blanket the continental US (Electromagnetic Pulse 2005). Open source materials have shown the US, China, France, and Russia all using an EMP burst as a surprise first strike in war games (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008; Winn 2008; Nock and Lizun 2007; Qian and Wang 1999). However, it is unlikely China would use such brute-force tactics. Using a high altitude atomic burst would cause international outrage as it violates an international treaty, it damages the environment, and it indiscriminately disrupts everything in its blast radius. Alternatively, shutting down the US power grid, production lines, water utilities, chemical plants, telecommunications, and transportation routes is possible through cyber attack, and it would provide the benefit of deniability. Details on how such an attack would be conducted are scarce in OSINT as governments do not wish to publicize their weaknesses or give away their assets. It is important however that they do acknowledge them, since any computer system which is connected to the internet is vulnerable to attack. In 2008, the CIA reported that multiple cities outside the US had their electrical power shut off by hackers. The reports were vague, supposedly due to security concerns; however it was reported that the attacks came from online, through the internet, not by physical means (Bridis 2008; McMillan 2008).

**Weapons of Mass Disruption**

OSINT continually points to cyber warfare being capable of crippling a state's electric power transmission, transportation systems, and communications systems (Phone Phreaking 2008; Weber 2008; Trahan 2008; McMillan 2007; Tkacik 2007; Reid 2007; Robson 2004; Miklaszewski 1999). If the Russian government was behind the cyber attacks on Estonia, it did not use such a dramatic assault. The Russians may simply have been testing their cyber warfare capabilities, saving their most devastating capability for when it is needed most, as it may only work once. Such an attack would cripple the flow of goods, effectively starving the population and shutting down business. Evidence that such a possibility exists can be seen across the globe. In 1997, a teenager shut down air and ground communication at a US airport in Massachusetts, and in 2000, the Russian government announced that hackers had succeeded in taking control of the world's largest natural gas pipeline network, Gazprom, by using a type of Trojan. In 2000, Vitek Boden took control of a sewage pumping station in Australia. He remotely triggered the release of a million litres of sewage into public waterways (Barker 2002). Computers and manuals seized in Al Qaeda training camps contained large amounts of SCADA information related to dams and critical infrastructure. In 2003, the Slammer Worm took a US nuclear power plant's safety monitoring system offline, and the Blaster Worm was connected with a massive blackout in the Eastern US (Maynor and Graham 2006).

The United States is particularly vulnerable as much of the communication, manufacturing, water, transportation, and energy infrastructure is owned by the private sector, as opposed to China and Russia where infrastructure is predominantly in the hands of the government (Greenemeier 2007). The relative ease with which the Titan Rain attacks were conducted make private sector computer networks look like an easy target (Almeida 2006). The government and defence installations are heavily funded for security, whereas the private sector is not. Initially the US power grid control systems were on closed networks (not connected to the internet). However, over time companies began deciding it was too costly to maintain separate networks. The internet became essential for operations, meaning they would need two separate systems for operation, one connected and one not. Through the decision-making process companies decided it was cheaper to have only the one that was

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

connected, but focus on keeping it secure. Over time security became lax, and no network that is connected can be entirely secure. Many of these systems do not support authentication, encryption, or basic validation protocols; of those that do support them, most run with security features disabled (Maynor and Graham 2006). In addition to the internet, SCADA systems may be compromised through outdated modems used for maintenance purposes, wireless access points, or roaming notebooks. Further, power companies may buy and trade power amongst themselves, so loopholes designed to check available capacity have provided another entry point (Winkler 2007). The vulnerability of the private sector's computer network, due to a lack of understanding or a lack of incentive, provides China (or other cyber-capable groups) with the opportunity to cripple US infrastructure.

**Point of Sale**

Using a modern fuel service station as a parallel for a cyber attack on commercial infrastructure, one can see the debilitating effects of a cyber attack. Magnetic stripe cards have replaced tangible notes as the primary method of payment. By overwhelming a bank through something as simple as a DDoS attack, an adversary could knock the point of sale banking system offline. Few service stations are equipped to handle this for duration longer than one day, and the Estonian attacks demonstrated a month-long capability. Lines in the store would grow as the speed of transactions dramatically slowed. Nearby ATMs would be taxed as people begin withdrawing more notes. As the ATM runs out of its supply of money, an internal alert is sent to notify the ATM provider to send an armoured car to restock the machine. This would require additional workflow, disrupting a fine tuned system of allocated staff hours and drivers. The long lines at the register would disrupt the productivity and efficiency of working customers who are unaccustomed to the long wait, and it would radiate frustration and anger throughout the community.

As the service line grows and employees struggle to keep up, the amount of store theft (fuel and merchandise) increases. More hours would be allocated to review surveillance footage, and the local police would be inundated with cases of theft. Panic may ensue, as seen with small disruptions at service stations, comparable to the temporary collapse of Optus telecommunications or the temporary collapse of Westpac banking (Streem 2008). A sustained disruption could lead to mob mentality. The fragility of social order was demonstrated in 2008 when fuel price increases led to widespread violent protests across the globe, including Argentina, Belgium, France, India, Indonesia, Malaysia, Portugal, South Korea, Spain, Thailand, and the UK (Arrests Following Jakarta Fuel Price Increases 2008; Banerjee and Zappei 2008; Cowell 2008; Fuel Demo Adds To Road Taxes Row 2008; Indonesia: Growing Fuel Price Protests Meet Repression 2008; Thai Truckers Join Global Fuel Price Protest 2008).

Alternatively, the registers themselves are operated by using the internet and could be targeted. China could bypass banking systems, energy providers, transportation systems, or communications systems and go after the less guarded, and less funded, point-of-sale software. Few service stations remain in the western world that use unconnected registers, as it would be difficult to remain competitive. Similarly, there are few competitors in the service station industry due to strong competition. This means there are only a small group of service station vendors within a large city, and all of the computers within those companies are running off of the same network. The six largest non-state owned energy companies, known as super majors, are: Exxon Mobil, Royal Dutch Shell, BP, Chevron Corporation, ConocoPhillips, and Total SA. These six companies control the vast majority of service



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

stations (SBDCNET 2001). This is sometimes obscured by the use of alternative store names, despite being contracted to a supermajor, or the continued use of an old company name despite having been bought out by a supermajor. This illustrates a lack of diversity in the retail industry. By attacking only a few targets, an entire city's service stations could be knocked offline. There are a limited number of independent operators within a typical city; however their numbers are too few to facilitate the influx of customers from the larger competitors.

Without the online register, PLUs (price look-up codes) cannot scan and prices would have to be manually added. Any extended duration of this process could shutdown a store, and depending on the system, fuel may not be able to be dispensed without the computer. Service stations are not known for their sophistication in computer defence as they routinely tighten budgets to their limits and they have not seen a need to harden this infrastructure. As community hostility rises, employees may resign due to stress. It would be difficult training new employees during this time with extended lines and the employees themselves suffering an inability to access fuel. New staff would also cause lost time and money for training. All delivery trucks create online invoices sent and received by the service station. Assuming they are able to maintain the fuel for their trucks, they would be forced to adapt to old methods of interaction and record keeping. A store's stock might also suffer shortages from hoarding of products due to panic in the community.

These systems could be attacked solely online, or operatives could be placed into the store to learn the system's weaknesses and install malware directly. Operations could be expanded beyond a service station to attack grocery and a wide range of retail outlets. Rather than going after the transport of goods, it may be easier to disrupt them online at their point of sale. The effects would radiate outward, knocking down additional infrastructure unable to handle the increased stress. A service station is only one example of weak commercial infrastructure that relies on computers to operate. If China could gain market dominance in the point of sale software industry, or in the registers used for sales, it would gain an even greater access to disruption. This disruption could be used as a deterrent, as blackmail, or as a force multiplier in traditional warfare.

**Market Dominance**

China may seek to establish market dominance in the production of ICT software and hardware as a means of increasing its cyber warfare capability. On an infrastructure level, China could seek to control ownership of submarine cable infrastructure allowing it further access to cyber reconnaissance or the option of shutting down portions of internet connectivity during times of war (Whitney 2008; Of Cables and Conspiracies 2008). Further, if China could unseat Microsoft as the industry standard in software, it could install backdoors, latent viruses, or remotely triggered ex-filtration devices. This type of tactic was examined in section 3, above (Cyber Reconnaissance and Attack), with Sony BMG's use of rootkits. China used legal and financial prowess to convince Microsoft to teach its software engineers how to insert their own software into Window's applications. As a part of the Chinese argument for doing so, was an insistence that Microsoft Windows was a secret tool of the US government. By providing China with "skeleton keys" to the Windows Operating System, inadvertently China was given advanced knowledge on how to infiltrate foreign computers and craft advanced exploits (Marsal 2008; Tkacik 2007).

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

US concerns over Chinese market dominance have begun to surface. In 2006, the State Department banned the purchase of computers from the Lenovo Group, the Chinese firm that acquired the IBM personal computing division, following penetrations using a zero-day flaw in Microsoft software. China is also growing in the field of microchips, something other states need for defence related electronics. Not only could China embed exploits, but also dominance in this field gives it access to critical individuals and information through partnership, such as a chance to liaise with industry insiders, come close to sensitive information and hardware, and conduct social engineering or HUMINT. In 2003, the Huawei Shenzhen Technology Company was charged with stealing secrets and wholesale pirating of Cisco software, a US company. In 2007, Huawei then attempted to buy 3Com, a US company which supplies the US government with security software, routers, and servers. India turned down a $60 million Huawei investment deal in 2005 after concerns over cyber reconnaissance, noting that Huawei is the same company that conducts sweeping and debugging of the Chinese embassy. India's Defence Ministry stated 'the choice was between cheap Chinese equipment and national security' (Tkacik 2007).

China consistently reverse engineers ICT hardware and software in an attempt to maintain a stronghold on its own markets. This can be seen with the reverse engineering of Skype Protocol and Voice over Internet Protocol (VoIP), and 'knock offs' of the iPhone (VoIP WkiBlog 2006). The One Laptop Per Child (OLPC) project, which has the potential to rapidly spread internet connectivity to China's remaining population, uses an open source operating system and software, helping to free China from US owned Microsoft. Yet China has denounced the sale of OLPC, promoting instead various domestic versions that were reversed engineered from the OLPC model. Further, the Chinese have secured manufacturing rights to produce OLPC within China even though they do not intend to promote OLPC sales domestically (O'Brien 2008). China also has a history of reverse engineering websites that become popular and profitable in the Western world; examples include clones of YouTube, Google, MySpace, Facebook, Wikipedia, and eBay being YoQoo, Baidu, Baidu Space, Xiaonei/Zhanzuo, Baidu Baike/Hoodong, and Taobao respectively (Marshall 2008; Wei 2008; Burns 2006).

**Peacetime Operations**

During peacetime, China is likely to rely on cyber reconnaissance to gather information and catalogue exploits/weaknesses in the US military and infrastructure. Automobile companies, food services, oil companies, financial institutions, and telecommunications all play a vital role in supporting military operations, as well as housing technological advances, expertise, and inside information which could prove useful for leapfrogging (Winkler 2005). Technology transfer allows China to skip years of costly research and development, and it removes the competitive edge of foreign militaries and companies (Tkacik 2007). In unrestricted fashion, China may also seek advantage during peacetime to battle military export restrictions of the EU, purchase vital capital in the US financial system, and help shape the international legal structure being developed for cyber warfare. Cyber reconnaissance against US military logistics networks could reveal force deployment information, such as the names of ships deployed, readiness status of various units, timing and destination of deployments, and rendezvous schedules. It could also reveal the details of weaponry sold to Taiwan.

China has repeatedly shown interest in the US Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) (China's Proliferation Practices, and the Development of Its



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

Cyber and Space Warfare Capabilities 2008). NIPRNet is used to exchange unclassified but sensitive information between internal users. The network is connected to the broader internet to improve collaboration between scientists and officers located in different organizations and in remote locations. This means it can provide intruders with data such as 'ballistic weapons research, aircraft and ship design, military payroll, personnel records, procurement, modelling of battlefield environments, and computer security research' (Lewis 1994). The US places classified military information on the Secret Internet Protocol Router Network (SIPRNet) and secret information on the Joint Worldwide Intelligence Communications System (JWICS). While these networks are not connected to the internet, examining NIPRNet may give insight into the contents through cross talk, or it may provide a means of escalating privileges, providing information on how to access SIPRNet and JWICS either directly or indirectly via an asset.

**Taiwan**

China can use the internet to manipulate the Taiwanese populace, either to set up for an attack, or to undermine Taiwan independence peacefully and avoid conflict altogether. This may include PSYOPS/propaganda, recruitment and identification of sympathizers, or cataloguing of cyber and defence weaknesses. For example, an internet rumour in 1999 that a Chinese Su-27 had shot down a Taiwan aircraft caused the Taipei stock market to drop more than two percent in less than four hours. An earthquake in 1999 and a typhoon in 2001 revealed weaknesses in Taiwan's telecommunications, electric power, and transportation infrastructure; weaknesses which could be targeted in physical sabotage. Further, a landslide revealed that the loss of a single power grid tower is capable of knocking out 90 percent of the power grid in the central mountainous region. Building information, including the location of the President's office, and daily activities, are openly available on the internet. This is even more significant given the lack of security present during the 2004 assassination attempt on President Chen Shui-bian and Vice President Annette Lu (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008; Taiwan Assassin 2004).

In the event of a Taiwan conflict, China could use cyber attacks to delay US involvement long enough for Taiwan to capitulate. For example, China could go after the US logistical apparatus, using information gained via NIPRNet, in order to delay the force deployment phase. This would include the organization of forces, food supplies, uniforms, and/or communication which are often organised through networks that are connected to the internet. Cyber attack could also delay re-supply to the region by misdirecting stores, fuel, and munitions, corrupting or deleting inventory files, and thereby hindering mission capability. If the Chinese lack the capability to find exploits in NIPRNet, they could simply conduct DDoS attacks to bring it down long enough for a Taiwanese surrender. While delaying the US, China could use traditional military forces in concert with cyber warfare against Taiwan. The cyber warfare component could include online PSYOPS, media warfare, special forces aided by cyber reconnaissance information, and cyber attacks against Taiwan's point of sale and banking infrastructure.

## 6. Conclusion

This research has shown that China seeks to leapfrog in military competitiveness by utilizing cyber warfare. Chinese military doctrine places an emphasis on asymmetric attack. Cyber

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

warfare epitomizes this a low cost means of levelling the playing field. Cyber attack strikes at a superior adversary's weakness – in the case of the US, a heavy reliance on hi-tech computerized weaponry and a civilian population reliant on an unsecured computer infrastructure. Cyber reconnaissance follows China's tradition of technology transfer and reverse engineering for domestic production as a means of leapfrogging. Cyber reconnaissance gives the added benefit of providing deniability, low cost, a lack of legal framework against it, and the removal of geographical distance. Foreign allegations, such as the Titan Rain incursions, suggest China is making rapid progress in cyber reconnaissance and attack capabilities. The PRC openly states in its National Defense White Paper that it is seeking informationization and modernization of the PLA. This follows the US, China's perceived greatest threat, in its pursuit of NCW, IO, and FCS. Cataloguing adversary weaknesses not only provides an asymmetric advantage in the event of a conflict, it also acts as a deterrent while China catches up in traditional military might. By utilizing cyber reconnaissance, China can accelerate its advancement in hi-tech weaponry. Unrestricted warfare has shown a blurring of the lines between military and non-military spheres. China can tap into the power of its online population for military purposes, such as seen in the Estonian, Georgian and Chanology case studies. Following the US example of IO, China can leverage the internet as a means of boosting soft power. Using cyber reconnaissance, the Chinese can gain market dominance in the fields of ICT. This will provide increased cyber security, by removing foreign influence, and it will provide improved cyber offence, such as pre-installed exploits or ownership of internet infrastructure. Market dominance also relates to financial gain, which China has stated is intrinsically related to military capabilities and strategic interests.

## References

Adams, Eric. 2004. Rods From God. Retrieved on March 10, 2008, from http://www.popsci.com/scitech/article/2004-06/rods-god.

Alberts, David S. 2002. Information Age Transformation. Retrieved on February 22, 2008, from http://www.dodccrp.org/files/Alberts_IAT.pdf.

Alberts, David S., Garstka, John J., Stein, Frederick P. 2000. Network Centric Warfare. Retrieved on February 2, 2008, from http://www.dodccrp.org/files/Alberts_NCW.pdf.

Allen, Kenneth. 2005. Reforms in the PLA Air Force. Retrieved on February 12, 2008, from http://www.jamestown.org/publications_details.php?volume_id=408&issue_id=3390&article_id=2369972.

Allen, Kenneth W., Glenn Krumel, Jonathan D. Pollack. 1995. China's Air Force Enters the 21st Century. Retrieved 1 February 2008, from http://www.rand.org/pubs/monograph_reports/2005/MR580.pdf.

Almeida, Marcelo. 2006. Cyberwar: The Beginning. Retrieved on March 3, 2008, from http://www.zone-h.org/index.php?option=com_content&task=view&id=13932&Itemid=30&msgid=710.

Annual Report to Congress: Military Power of the People's Republic of China 2008. 2008. Retrieved on March 15, 2008, from http://www.globalsecurity.org/military/library/report/2008/2008-prc-military-power.htm.

Annual Report to Congress: Military Power of the People's Republic of China 2007. 2007. Retrieved on February 18, 2008, from http://www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf.

A Cyber-Riot. 2007. Retrieved on February 2, 2008, from http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598.

Amnesty International. 2004. People's Republic of China Controls tighten as Internet activism grows. Retrieved on August 1, 2008, from http://www.amnesty.org/en/library/asset/ASA17/001/2004/en/dom-ASA170012004en.html.

Appel, Edward. 2004. China's Espionage: What's At Stake. Retrieved on March 20, 2008, from http://www.pbs.org/wgbh/pages/frontline/shows/spy/spies/atstake.html.



Published by ePublications@bond, 2008

Armoured Fighting Vehicles. 2008. Retrieved on April, 10, 2008, from http://www.sinodefence.com/army/armour/default.asp.
Arrests Following Jakarta Fuel Price Increases. 2008. Retrieved on August 1, 2008, from http://www.radioaustralia.net.au/news/stories/200806/s2285064.htm.
Baard, Mark. 2007. Sentient World: War Games on the Grandest Scale. Retrieved on March 20, 2008, from http://www.theregister.co.uk/2007/06/23/sentient_worlds/.
Banerjee, Manik and Zappei, Julia. 2008. Fuel Price Hikes Spark Protests In India And Malaysia That Could Undermine Governments. Retrieved on August 1, 2008, from http://www.aol.com.au/news/story/Fuel-price-hikes-spark-protests-in-India-and-Malaysia-that-could-undermine-governments/550071/index.html.
Barker, Garry. 2002. Cyber terrorism a mouse-click away. Retrieved on February 24, 2008, from http://www.theage.com.au/articles/2002/07/07/1025667089019.html.
Basu, Indrajit. 2008. India Faces Cyber Challenge From China. Retrieved on June 10, 2008, from http://www.upiasiaonline.com/Security/2008/05/09/india_faces_cyber_challenge_from_china/5587/.
Beam It Right There Scotty. 2005. Retrieved on January 26, 2008, from http://www.wired.com/science/discoveries/news/2005/07/68152.
Berkeley Bionics Human Exoskeleton. 2007. Retrieved On March 10, 2008, from http://www.youtube.com/watch?v=EdK2y3lphmE.
Block, Ryan. 2006. The Brain Port, Neural Tongue Interface Of The Future. Retrieved on March 10, 2008, from http://www.engadget.com/2006/04/25/the-brain-port-neural-tongue-interface-of-the-future/.
Bloom, James. 2008. Robots ready to support soldiers on the battlefield. Retrieved on June 26, 2008, from http://www.guardian.co.uk/technology/2008/jun/26/robots.weapons technology.
Bonsor, Kevin. 2008. How Augmented Reality Will Work. Retrieved on March 10, 2008, from http://www.howstuffworks.com/augmented-reality.htm.
Boyd, Clark. 2008. Profile: Gary McKinnon. Retrieved on August 4, 2008, from http://news.bbc.co.uk/2/hi/technology/4715612.stm.
Bradsher, Keith. 2006. Hong Kong enlists youth to fight piracy. Retrieved on July 20, 2008, from http://www.iht.com/articles/2006/07/18/business/piracy.php.
Braukus, Michael. 2004. NASA Develops System To Computerize Silent Subvocal Speech. Retrieved on March 2008, from http://www.nasa.gov/home/hqnews/2004/mar/HQ_04093_subvocal_speech.html.
Brenner, Bill. 2007. Experts doubt Russian government launched DDoS attacks. Retrieved on February 18, 2008, from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1255548,00.html.
Bingemann, Mitchell. 2008. Buggy Software Sends Optus Offline. Retrieved on August 8, 2008, from http://www.australianit.news.com.au/story/0,,24141034-15306,00.html.
Brenner, Bill. 2005. Myfip's Titan Rain Connection. Retrieved on January 8, 2008, from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1120855,00.html.
Bridis, Ted. 2008. CIA: Hackers demanding cash disrupted power. Retrieved on February 2, 2008, from http://www.msnbc.msn.com/id/22734229/.
Bright, Arthur. 2007. Estonia Accuses Russia Of Cyberattack. Retrieved on March 10, 2008, from http://www.csmonitor.com/2007/0517/p99s01-duts.html.
Brookes, Peter. 2006. China's Influence In Africa. Retrieved on March 15, 2008, from http://www.heritage.org/Research/AsiaandthePacific/bg1916.cfm.
Bruno, Greg. 2008. The Evolution of Cyber Warfare. Retrieved on March 12, 2008, from http://www.cfr.org/publication/15577/.
Burns, Simon. 2006. MySpace and Wikipedia Clones Storm China. Retrieved on July 31, 2008, from http://www.itnews.com.au/News/NewsStory.aspx?story=35422.
Center for Strategic and International Studies. 2003. China's Space Program. Retrieved on April 3, 2008, from http://www.csis.org/index.php?option=com_csis_progj&task=view&id=76.
China and Internet Censorship. 2006. Retrieved on August 5, 2008, from http://www.cnn.com/interactive/world/0603/explainer.china.internet/frameset.exclude.html.
China defends internet regulation. 2006. Retrieved on July 15, 2008, from http://news.bbc.co.uk/2/hi/asia-pacific/4715044.stm.
China hires Net squad to sway opinion. 2005. Retrieved on July 15, 2008, from http://www.asiamedia.ucla.edu/article.asp?parentid=24609.
China internet use grows. 2006. Retrieved on August 1, 2008, from http://news.bbc.co.uk/

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

2/hi/business/2145865.stm.
China Tightens Vice On Internet. 2006. Retrieved on June 11, 2008, from http://cryptome.cn/china-vise.htm.
China's National Defense in 2006 (White Paper). 2006. Retrieved on March 3, 2006, from http://www.fas.org/nuke/guide/china/doctrine/wp2006.html.
China's Navy 2007. 2007. US Office of Naval Intelligence. Retrieved January 10, 2008, from http://fas.org/irp/agency/oni/chinanavy2007.pdf.
China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities. 2008. Retrieved on June 30, 2008, from http://www.uscc.gov/hearings/2008hearings/transcripts/08_05_20_trans/08_05_20_trans.pdf.
China's Space Program Aims at Peaceful Use of Space Resources. 2005. Chinanews.cn, 15 October. Retrieved on July 10, 2006, from www.chinanews.cn/news/2005/2005-10-15/12428.html
Chinese Submarines. 2008. Retrieved on April 10, 2008, from http://www.sinodefence.com/navy/sub/default.asp.
Christensen, John. 1999. Bracing For Guerrilla Warfare In Cyberspace. Retrieved on February 2, 2008, from http://edition.cnn.com/TECH/specials/hackers/cyberterror/.
Code Red Worm Spreading, Set To Flood Whitehouse. 2001. Retrieved on July 18, 2008, from http://slashdot.org/articles/01/07/19/2230246.shtml.
Cost of Code Red Rising. 2001. Retrieved on February 2, 2008, from http://archives.cnn.com/2001/TECH/internet/08/08/code.red.II/.
Coleman, Kevin. 2008. Cyber War 2.0 – Russia V. Georgia. Retrieved on August 13, 2008, from http://www.defensetech.org/archives/004363.html.
Commissar of Nashi says he waged cyber attack on Estonian government sites. 2007. Retrieved on March 10, 2008, from http://www.sbcc-chamber.com/index.php?lng=en&page_id=60&news_id=888.
Cook, John. 2008. Cult Friction. Retrieved on July 14, 2008, from http://www.radaronline.com/from-the-magazine/2008/03/scientology_anonymous_protests_tom_cruise_01.php.
Cooper, Simon. 2006. How China Steals US Military Secrets. Retrieved on April 2, 2008, from http://www.popularmechanics.com/technology/military_law/3319656.html.
Cordesman, Anthony, and Kleiber, Martin. 2006. Overview of Major Asians Powers. Retrieved on March 12, 2008, from http://www.csis.org/media/csis/pubs/060626_asia_balance_powers.pdf.
Corpus, Victor N. 2006. Americas Acupuncture Points, Part 1. Retrieved on March 18, 2008, from http://www.atimes.com/atimes/China/HJ19Ad01.html.
Corpus, Victor N. 2006. Americas Acupuncture Points, Part 2. Retrieved on March 18, 2008, from http://www.atimes.com/atimes/china/HJ20Ad01.html.
Cowell, Alan. 2008. French Truckers Protest Fuel Prices. Retrieved on August 1, 2008, from http://www.nytimes.com/2008/06/17/world/europe/17fuel.html.
Cox Report. 1999. Retrieved on June 12, 2008, from http://www.fas.org/spp/starwars/congress/1999_r/cox/ch1bod.htm.
Cuban, Brian. 2008. Confessions of a Banned Digger. Retrieved on September 5, 2008, from http://www.briancuban.com/confessions-of-a-banned-digger/.
Cyberwarfare in International Law. 2008. Retrieved on March 8, 2008, from http://yro.slashdot.org/article.pl?no_d2=1&sid=08/01/24/2151233.
Davidson, Keay. 2004. Air Force Pursuing Antimatter Weapons. Retrieved on March 10, 2008, from http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/10/04/MNGM393GPK1.DTL.
Delio, Michelle. 2001. Code Blue Targets China Firm. Retrieved on February 10, 2008, from http://www.wired.com/science/discoveries/news/2001/09/46624.
Delio, Michelle. 2001. It's Cyber War: China vs. US. Retrieved on July 2, 2008, from http://www.wired.com/politics/law/news/2001/04/43437.
Derene, Glenn. 2008. Inside NSA Red Team Secret Ops with Government's Top Hackers. Retrieved on August 10, 2008, from http://www.popularmechanics.com/technology/military_law/4270420.html.
Dick, Stevens J. 2006. The Importance of Exploration. Retrieved on March 3, 2008, from http://www.nasa.gov/missions/solarsystem/Why_We_01pt1.html.
DoS Attacks on Estonia Were Launched by Student. Retrieved on March 8, 2008, from http://politics.slashdot.org/article.pl?no_d2=1&sid=08/01/25/0120221.
Economy, Elizabeth C. And Segal, Adam. 2008. China's Olympic Nightmare. Retrieved on June 30, 2008, from http://www.foreignaffairs.org/20080701faessay87403-p0/elizabeth-

c-economy-adam-segal/china-s-olympic-nightmare.html.
Espiner, Tom. 2006. Academics break the Great Firewall of China. Retrieved on July 4, 2008, from http://news.com.com/2100-7348_3-6090437.html?part=rss&tag=6090437&subj=news.
Espiner, Tom. 2005. Security Experts Lift Lid On Chinese Hack Attacks. Retrieved on February 9, 2008, from http://news.zdnet.com/2100-1009_22-5969516.html.
Estonia Fines Man for Cyber War. 2008. Retrieved on February 12, 2008, from http://news.bbc.co.uk/2/hi/technology/7208511.stm.
Estonia Has No Evidence of Kremlin Involvement. 2007. Retrieved on March 10, 2008, from http://en.rian.ru/world/20070906/76959190.html.
Estonia Hit by Moscow Cyber War. 2007. Retrieved on January 23, 2008, from http://news.bbc.co.uk/2/hi/europe/6665145.stm.
Everett, Margaret. Latin America On-line: The Internet, Development, and Democratization. 1998. Retrieved on March 2, 2008, from http://library.nmsu.edu/subject/bord/laguia/everett.html.
Faiola, Anthony. 2005. Anti-Japanese Hostilities Move to the Internet. Retrieved on June 8, 2008, from http://www.washingtonpost.com/wp-dyn/content/article/2005/05/09/AR2005050901119.html.
FCS Watch. Retrieved on March 10, 2008, from http://www.defensetech.org/archives/cat_fcs_watch.html.
French, Howard W. 2006. Chinese Tech Buffs Slake Thirst for U.S. TV Shows. Retrieved on August 4, 2008, from http://www.nytimes.com/2006/08/09/world/asia/09china.html/partner/rssnyt?_r=2&oref=slogin.
Friedman, Elisabeth Jay. 2005. The Reality of Virtual Reality. Retrieved February 22, 2008, from http://programs.ssrc.org/itic/publications/friedman.pdf.
Fuel Demo Adds to Road Taxes Row. 2008. Retrieved on August 1, 2008, from http://news.bbc.co.uk/2/hi/uk_news/7420792.stm.
Future Combat Systems. 2008. Retrieved on March 10, 2008, from http://www.globalsecurity.org/military/systems/ground/fcs.htm.
Gannon, John C. 2001. The National Security Telecommunications and Information Systems Security Committee. Retrieved on February 12, 2008, from http://www.dni.gov/nic/speeches_telecommunications.html.
General Staff Department. 1997. Retrieved on March 20, 2008, from http://www.fas.org/irp/world/china/pla/gen_staff.htm.
GOA. 1996. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Retrieved on February 5, 2008, from http://www.fas.org/irp/gao/aim96084.htm.
Goodin, Dan. 2008. India and Belgium Decry Chinese Cyber Attacks. Retrieved on June 10, 2008, from http://www.theregister.co.uk/2008/05/08/belgium_india_china_warnings/.
Google censors itself for China. 2006. Retrieved on July 22, 2006, from http://news.bbc.co.uk/2/hi/technology/4645596.stm.
Graham, Bradley. 2005. Hackers Attack Via Chinese Websites. Retrieved on January 8, 2008, from http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.
Greenberg, Andy. 2007. Apples For The Army. Retrieved on January 20, 2008, from http://www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx_ag_1221army.html.
Greenberg, Andy. 2007. Worst Cybersecurity Meltdowns. Retrieved on February 18, 2008, from http://www.forbes.com/2007/10/26/tjx-northrop-mcafee-ent-tech-cx_ag_1026worsthacks.html.
Greenemeier, Larry. 2007. China's Cyber Attacks Signal New Battlefield Is Online. Retrieved on July 7, 2008, from http://www.sciam.com/article.cfm?id=chinas-cyber-attacks-sign.
Grier, Peter. 2005. Spy Case Patterns The Chinese Style of Espionage. Retrieved on March 23, 2008, from http://www.csmonitor.com/2005/1130/p01s01-usfp.html.
Griggs, Brandon. 2008. US at risk of Cyberattacks, Experts Say. Retrived on August 25, 2008, from http://edition.cnn.com/2008/TECH/08/18/cyber.warfare/index.html.
Hacker Attacks in US Linked to Chinese Military. 2005. Retrieved on July 21, 2006, from http://www.breitbart.com/news/2005/12/12/051212224756.jwmkvntb.html.
Hacking Textfiles. 2008. Retrieved on June 8, 2008, from http://www.textfiles.com/hacking/.

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

Hacking US Government Computers from Overseas. 2001. Retrieved on February 2, 2008, from http://www.totse.com/en/hack/understanding_the_internet/163724.html.

Hanson, Stephanie. 2008. China, Africa, and Oil. Retrieved on June 12, 2008, from http://www.cfr.org/publication/9557/.

Ha, Michael. 2008. China Gateway for Most Cyber-Attacks. Retrieved on June 20, 2008, from http://www.koreatimes.co.kr/www/news/nation/2008/05/116_24499.html.

Heilemann, John. 2006. How Digg.com is Democratizing the News. Retrieved on March 27, 2007 from http://money.cnn.com/2006/03/24/magazines/business2/diggdemocratizes/index.htm.

Hershkovitch, Ady. 1998. Plasma Window Technology for Propagating Particle Beams and Radiation from Vacuum to Atmosphere. Retrieved on March 10, 2008, from http://www.techbriefs.com/content/view/1834/32/1/0/.

Hi-tech Thieves Target Olympics. 2008. Retrieved on August 20, 2008, from http://news.bbc.co.uk/2/hi/technology/7548870.stm.

Hill, John. 2004. China's Assassin's Mace Meets The Taiwanese Scorpion. Retrieved on March, 18, 2008, from http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1044.

Hines, Matt. 2008. Be prepared: ActiveX attacks will persist. Retrieved on March 10, 2008, from http://www.infoworld.com/article/08/02/19/08NF-activex-horror_1.html.

Hollis, Duncan. Why States Need an International Law For Information Operations. Retrieved on March 2, 2008, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1083889.

Ikenberry, John G. 2008. The Rise of China and the Future of the West. Retrieved on February 10, 2008, from http://www.foreignaffairs.org/20080101faessay87102-p0/g-john-ikenberry/the-rise-of-china-and-the-future-of-the-west.html.

Indonesia: Growing Fuel Price Protest Meet Repression. 2008. Retrieved on August 1, 2008, from http://www.greenleft.org.au/2008/752/38852.

Information Operations Roadmap. 2003. Declassified US Government document. Retrieved on March 1, 2008, from http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

International Assessment and Strategy Center. 2005. Top Ten Chinese Military Modernization Developments. Retrieved on February 15, 2008, from http://www.strategycenter.net/research/pubID.65/pub_detail.asp.

International Institute for Strategic Studies. 2008. The Military Balance 2008. Routledge for IISS, Abingdon.

Internet censorship in the People's Republic of China. 2006. Retrieved on August 2, 2008, from http://en.wikipedia.org/wiki/The_Great_Firewall

Internet Filtering in China in 2004-2005. 2005. Retrieved on July 21, 2008, from http://opennet.net/studies/china.

Internet Group Declares War on Scientology. Retrieved on March 8, 2008, from http://yro.slashdot.org/article.pl?no_d2=1&sid=08/01/24/1311252.

Iran Missile Test Provocative. 2008. Retrieved on August 2, 2008, from http://news.bbc.co.uk/2/hi/middle_east/7498214.stm.

Isachenkov, Vladimir. 2007. Russian Space Exec Convicted For Aiding China. Retrieved on March 10, 2008, from http://www.msnbc.msn.com/id/22082431/.

ISN. 2001. Code Red virus probably began in China. Retrieved on July 18, 2006, from http://www.landfield.com/isn/mail-archive/2001/Sep/0007.html.

Jesdanun, Anick. 2008. Chinese Internet Users Up to 210 Million. Retrieved on February 20, 2008, from http://www.physorg.com/news119947914.html.

Johnston, Alastair. 2002. Toward Contextualizing the Concept of a Shashoujian (Assassin's Mace). Retrieved on February 24, 2008, from http://www.people.fas.harvard.edu/~johnston/shashoujian.pdf.

Jordan, Jakes. 2008. US Charges 2 In China Spy Case. Retrieved on April 1, 2008, from http://www.time.com/time/world/article/0,8599,1726799,00.html.

Kiezer, Gregg. 2005. Dutch Botnet Suspects Ran 1.5 Million Machines. Retrieved on August 1, 2008, from http://www.techweb.com/wire/security/172303160.

Kerner, Sean. 2007. Estonia Under Russian Cyber Attack? Retrieved on February 19, 2008, from http://www.internetnews.com/security/article.php/3678606.

Klein, Alec. 2007. The Army's $200 Billion Makeover. Retrieved on March 10, 2008, from http://www.washingtonpost.com/wp-dyn/content/story/2007/12/06/ST2007120602927.html.



Published by ePublications@bond, 2008

Kumar, T. 2006. Human Rights and the Internet in China. Retrieved on August 4, 2008, from http://www.amnestyusa.org/document.php?id=ENGUSA20060201001.

Lam, Willy Wo-lap. 2004. Beijing's New "Balanced" Foreign Policy: An Assessment. China Brief, Vol. 4, No. 4, 20 February. The Jamestown Foundation, Retrieved on February 6, 2006, from http://www.jamestown.org/publications_details.php?volume_id=395&&issue_id=2912

Landler, Mark and Markoff, John. 2007. Digital Fears Emerge After Data Siege in Estonia Retrieved on February 2, 2008, from http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=2&ref=technology&oref=slogin&oref=slogin.

Lasker, John. 2005. US Military's Elite Hacker Crew. Retrieved on February 18, 2008, from http://www.wired.com/politics/security/news/2005/04/67223.

Layer 8. 2007. Did her MySpace photo derail teacher's career? Retrieved on June 18, 2008, from http://www.networkworld.com/community/?q=node/14584.

Lemon, Sumner. 2008. China Crafts Cyber Weapons. Retrieved on June 2, 2008, from http://www.pcworld.com/article/132284/china_crafts_cyberweapons.html.

Lemon, Sumner. 2007. Chinese Police Arrest Eight For Computer Virus. Retrieved on March 20, 2008, from http://www.infoworld.com/article/07/02/13/HNchinesearresteight_1.html.

Lewis, Jeffrey. 2005. Autonomous Nanosatellite Guardian For Evaluating Local Space (ANGELS). Retrieved on March 10, 2008, from http://www.defensetech.org/archives/001996.html.

Lewis, Peter. 1994. Computer Snoopers Imperil Pentagon Files, Experts Say. Retrieved on July, 2, 2008, from http://query.nytimes.com/gst/fullpage.html?res=9F04E3DD143EF932A15754C0A962958260.

Leyden, John. 2007. France blames China for hack attacks. Retrieved on January 2, 2008, from http://www.theregister.co.uk/2007/09/12/french_cyberattacks/.

Leyden, John. 2004. Telenor Takes Down Massive Botnet. Retrieved on August 1, 2008 from http://www.theregister.co.uk/2004/09/09/telenor_botnet_dismantled/.

Leyden, John. 2001. Code Blue Targets Red China. Retrieved on July 18, 2006, from http://www.theregister.co.uk/2001/09/10/code_blue_targets_red_china/.

Levinson, Charles. 2008. Hackers Attack Iraq's Vulnerable Computers. Retrieved on August, 25, 2008, from http://abcnews.go.com/Technology/story?id=5685746&page=1.

Liedtke, Michael. 2005. Google Agrees to Censor Results in China. Retrieved on July 22, 2006, from http://www.breitbart.com/news/2006/01/24/D8FBC4C02.html.

List of Internet Phenomena. 2008. Retrieved on April 10, 2008, from http://en.wikipedia.org/wiki/List_of_Internet_phenomena.

Lo, Joseph. 1996. Internet Chat Relay FAQ. Retrieved on March 15, 2006, from http://irchelp.org/irchelp/altircfaq.html.

Luard, Tim. 2005. China's Spies Come Out From The Cold. Retrieved on April 2, 2008, from http://news.bbc.co.uk/2/hi/asia-pacific/4704691.stm.

Lynch, David. 2007. Law Enforcement Struggles To Combat Chinese Spying. Retrieved on March 23, 2008, from http://www.usatoday.com/money/world/2007-07-22-china-spy-1_N.htm.

Malone, Scott. 2008. Hackers stole 40 million credit card numbers. Retrieved on August 10, 2008, from http://www.australianit.news.com.au/story/0,24897,24136467-15306,00.html.

Marshall, Matt. 2008. Xiaonei, The Facebook Of China, Raises $430M. Retrieved on April 2, 2008, from http://venturebeat.com/2008/04/30/xiaonei-the-facebook-of-china-raises-430m-better-funded-than-facebook/.

Magnuson, Stew. 2006. Wikipedia for Intel Officers Proves Useful. Retrieved on July 7, from http://www.allbusiness.com/public-administration/national-security-international/3932331-1.html.

Mao, Tse-Tung [Zedong]. 2000. On Guerrilla Warfare (trans. Samuel B. Griffith). Chicago: University of Illinois Press

Mark, David. 2008. Scientists one step closer to invisibility cloak. Retrieved on August 12, 2008, from http://www.abc.net.au/news/stories/2008/08/11/2330897.htm.

Marquand, Robert. 2007. China Emerges As Leader In Cyber Warfare. Retrieved on April, 10, 2008, from http://www.csmonitor.com/2007/0914/p01s01-woap.html.

Marsal, Katie. 2008. China asking Apple to intentionally cripple iPhones. Retrieved on September 26, 2008, from http://www.appleinsider.com/articles/08/09/25/china_mobile_asking_apple_to_intentionally_cripple_iphones.html.

Maynor, David and Graham, Robert. 2006. SCADA Security and Terrorism: We're Not

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

Crying Wolf. Retrieved on February 27, 2008, from http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.
McLaughlin, Martin. 1999. China Spy Scare. Retrieved on March 23, 2008, from http://www.wsws.org/articles/1999/mar1999/chin-m10.shtml.
McLean, Doug. 1995. Hacking in 17 Easy Steps. Retrieved on January 15, 2008, from http://web.archive.org/web/20010708111438/http://www.claws-and-paws.com/personal/hacking/17steps.shtml.
McMillan, Robert. 2008. CIA Says Hackers Have Cut Power Grid. Retrieved on January 19, 2008, from http://www.pcworld.com/article/id,141564-pg,1/article.html.
McMillan, Robert. 2008. Hackers Hit Scientology With Online Attack. Retrieved on July 14, 2008, from http://www.pcworld.com/article/141839/hackers_hit_scientology_with_online_attack.html.
McMillan, Robert. 2007. Couple Swarmed By SWAT Team After 911 Hack. Retrieved on June 7, 2008, from http://www.macworld.com/article/60576/2007/10/swat.html.
Miklaszewski, Jim. 1999. Pentagon and Hackers in Cyberwar. Retrieved on February 2, 2008, from http://news.zdnet.com/2100-9595_22-513930.html.
Milchman, Eli. 2006. Yahoo 'Strictest' Censor in China.Retrieved on July 15, 2006, from http://www.wired.com/news/technology/internet/0,71166-0.html?tw=rss.index.
Miller, Chuck 2008. The Rustock botnet spams again, SC Magazine July 25, from http://www.scmagazineus.com/The-Rustock-botnet-spams-again/article/112940/

Ministry of Internal Affairs Lists PMR's 10 Most Wanted. 2007. Retrieved on March 10, 2008, from http://www.tiraspoltimes.com/news/ministry_of_internal_affairs_lists_pmrs_10_most_wanted.html.

Missiles and Space Programme. 2008. Retrieved on March 20, 2008, from http://sinodefence.com/strategic/default.asp

Moore, Frank W. China's Military Capabilities. 2000. Retrieved on February 18, 2008, from http://www.comw.org/cmp/fulltext/iddschina.html.

Moss, William. 2006. Chinese YouTubes courting controversy. Retrieved on July 20, 2006, from http://asia.cnet.com/reviews/blog/littleredblog/0,39056119,39375940,00.htm.

Musharbash, Yassin. 2008. Insights Into The Cyber-Jihad. Retrieved on August 30, 2008, from http://www.spiegel.de/international/world/0,1518,575276,00.html.
Navrozov, Lev. 2005. Chinese Geostrategy: The Assassin's Mace. Retrieved on February 10, 2008, from http://archive.newsmax.com/archives/articles/2005/10/20/172811.shtml.
Newhouse, Barry. 2006. Group Accuses Internet Companies in China of Rights Violations. Retrieved on July 21, 2006, from http://www.voanews.com/english/2006-07-20-voa16.cfm.
New Technology Can Be Operated By Thought. 2007. Retrieved on March 10, 2008, from http://www.sciencedaily.com/releases/2007/11/071107210708.htm.
Nock, Howard and Lizun, Daniel. 2007. Cyberterrorism and Cybercrime: Are You Prepared. Retrieved on January 28, 2008, from http://www.clevelandfed.org/bsr/Conditions/v3n2/v3n2.htm.
Norton-Taylor, Richard. 2007. Titan Rain: How Chinese Hackers Targeted Whitehall. Retrieved on January 8, 2008, from http://www.guardian.co.uk/technology/2007/sep/04/news.internet.
Nuclear Electromagnetic Pulse. 2005. Retrieved on August 23, 2008, from http://cryptome.org/bartlett-060905.txt.
O'Brien, Kevin. 2008. OLPC XO Review and Teardown. Retrieved on January 14, 2008, from http://www.notebookreview.com/default.asp?newsID=4199.
O'Connell, Kelly. 2008. Internet Law: Hackers Disable Scientology Website & Declare War. Retrieved on July 14, 2008, from http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1972.
Of Cables and Conspiracies. 2008. Retrieved on July 4, 2008, from http://www.economist.com/world/international/displaystory.cfm?story_id=10653963.
Oliver, Chris. 2008. China's foreign exchange reserves jump 61.6 bln in January. Retrieved on March 13, 2008, from http://www.marketwatch.com/news/story/chinas-foreign-exchange-reserves-jump/story.aspx?guid=%7BEBE6E206-9BE9-4329-B71A-2AF2F903A5AD%7D.

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

Onley, Dawn and Wait, Patience. 2006. Red Storm Rising. Retrieved on January 8, 2008, from http://www.gcn.com/print/25_25/41716-1.html.

Operation Spam Zombies. 2005. Retrieved on August 1, 2008, from http://www.ftc.gov/bcp/conline/edcams/spam/zombie/partners.htm.

Pang, Kevin. 2008. Chinese text-message primer. Retrieved on August 25, 2008, from http://www.chicagotribune.com/features/lifestyle/chi-chinese.text.0812aug12,0,606145.story.

Paramilitary Olympics: Beijing: at least 94,000 security staff – but only 10,500 athletes. 2008. The Independent, April 13. Retrieved on September 20, 2008, from http://www.independent.co.uk/news/world/asia/paramilitary-olympics-beijing-at-least-94000-security-staff-ndash-but-only-10500-athletes-808490.html.

Pasternack, Alex. 2008. When Nature Won't Cooperate in China, Photoshop! Retrieved on April 10, 2008, from http://www.treehugger.com/files/2008/02/fake_photo_tibet_railway_antelope_greenwashing.php.

Paul, Ryan. 2007. Top US government research labs infiltrated by hackers. Retrieved on February 10, 2008, from http://arstechnica.com/news.ars/post/20071209-top-us-military-research-labs-infiltrated-by-hackers.html.

People's Daily Online. 2006. Authorities make first hit in anti-piracy campaign. Retrieved on July 29, 2008, from http://english.people.com.cn/200607/29/eng20060729_288072.html.

People's Armed Police. 2005. Retrieved on March 20, 2008, from http://www.globalsecurity.org/intell/world/china/pap.htm.

People's Armed Police Force Organisation. 2007. Retrieved on March 20, 2008, from http://www.sinodefence.com/organisation/armedpolice/introduction.asp.

Phone Phreaking. 2008. Retrieved on June 26, 2008, from http://www.textfiles.com/phreak/.

Pike, John. 2008. China's Defense Budget. Retrieved on February 2, 2008, from http://www.globalsecurity.org/military/world/china/budget.htm.

Pike, John. 2008. X-45 Unmanned Combat Air Vehicle (UCAV). Retrieved on August 10, 2008, from http://www.fas.org/man/dod-101/sys/ac/ucav.htm.

Pillsbury, Michael. 2000. China Debates the Future Security Environment. National Defense University Press. Retrieved on February 2, 2008, from http://www.fas.org/nuke/guide/china/doctrine/pills2/part08.htm.

Pirates of the Orient. 2006. Retrieved on July 15, 2008, from http://www.thestandard.com.hk/weekend_news_detail.asp?pp_cat=30&art_id=22887&sid=8816949&con_type=3&d_str=20060715.

Polyanskaya, Anna. 2006. Commissars of the Internet. Retrieved on June 12, 2008, from http://lrtranslations.blogspot.com/2007/02/commissars-of-internet.html.

PRC Acquisitions of US Technology. 1998. Retrieved on March 10, 2008, from http://www.fas.org/spp/starwars/congress/1999_r/cox/ch1bod.htm.

Put Your Mobile Where Your Mouth Is. 2002. Retrieved on March 10, 2008, from http://news.bbc.co.uk/2/hi/science/nature/2055654.stm.

Qiao, Liang and Wang Xiangsui. 1999. Unrestricted Warfare. Retrieved on February 10, 2008, from http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf

Raduege, Harry. 2004. Net-Centric Warfare Is Changing The Battlefield Environment. Retrieved on April 2, 2008, from http://www.stsc.hill.af.mil/crosstalk/2004/01/0401Raduege.html.

Ramadge, Andrew. 2008. Scientology protest surge crashes websites. Retrieved on July 14, 2008, from http://www.news.com.au/technology/story/0,25642,23212002-5014239,00.html.

Raun, Alo. 2007. Venemaa jätab Eesti küberrünnakute uurimisel õigusabita. Retrieved on March 10, 2008, from http://www.postimees.ee/060707/esileht/siseuudised/270899.php.

Reid, Tim. 2007. China's cyber army is preparing to march on America, says Pentagon. Retrieved on February 21, 2008, from http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece.

Reporters Without Borders. 2006. Yahoo ! implicated in third cyberdissident trial. Retrieved on July 25, 2008, from http://www.rsf.org/article.php3?id_article=17180.

Richards, Jonathan. 2008. China Blocks YouTube Yahoo! Over Tibet. Retrieved on March 12, 2008, from http://technology.timesonline.co.uk/tol/news/tech_and_web/article3568040.ece.

Robson, Gary. 2004. The Origins of Phreaking. Retrieved on June 28, 2008, from http://www.robson.org/gary/writing/phreaking.html.

SBDCNET. 2001. Convenience Store/Gasoline Station Market Profile. Retrieved on June 1,

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

2008, from http://sbdcnet.utsa.edu/industry/gas_stations.pdf.
Schearf, Daniel. 2006. Chinese Intellectuals Condemn Web Site Closure. Retrieved on August 4, 2008, from http://www.voanews.com/english/2006-08-04-voa17.cfm.
Second Artillery Corps. 2000. Retrieved on March 20, 2008, from http://www.fas.org/nuke/guide/china/agency/2-corps.htm.
Second Intelligence Department. 2005. Retrieved on March 24, 2008, from http://www.globalsecurity.org/intell/world/china/pla-dept_2.htm.
Schwartz, John. 2007. When Computers Attack. Retrieved on February 2, 2008, from http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html?_r=1&oref=slogin.
Shaughnessy, Larry. 2008. CIA, FBI push Facebook for Spies. Retrieved on September 5, 2008, from http://edition.cnn.com/2008/TECH/ptech/09/05/facebook.spies/index.html?eref=rss_latest.
Single, Ryan. 2008. War Breaks Out Between Hackers And Scientology. Retrieved on July 14, 2008, from http://blog.wired.com/27bstroke6/2008/01/anonymous-attac.html.
Skype Protocol Has Been Cracked. 2006. Retrieved on July 14, 2008, from http://politics.slashdot.org/article.pl?sid=06/07/14/1514226.
Slashdot Subculture. 2008. Retrieved on April 10, 2008, from http://wikipedia.qwika.com/en/Slashdot_subculture.
Slashdot Trolling Phenomenon. 2008. Retrieved on April 10, 2008, from http://wikipedia.qwika.com/en/Slashdot_trolling_phenomena.
Small Arms. 2008. Retrieved on April 10, 2008, from http://www.sinodefence.com/army/small_arms/default.asp.
Smith, Charles. 2001. Russian Rocket Torpedo Arms Chinese Subs. Retrieved on February 10, 2008, from http://archive.newsmax.com/archives/articles/2001/4/23/220813.shtml.
Sobrale, Saada. 2007. Venemaa keeldus koostööst küberrünnakute uurimisel. Retrieved on March 10, 2008, from http://www.epl.ee/artikkel/392271.
Streem. 2008. Westpac Glitch Leaves Customers Cashless. Retrieved on August 13, 2008, from http://www.streem.com.au/breaking-news/6326-thousands-blocked-as-westpac-crashes.
Sun Tzu [Zi]. 1963. *The Art of War* (trans. Samuel B. Griffith). London: Oxford University Press.
Surface Combatants. 2008. Retrieved on April 9, 2008, from http://www.sinodefence.com/navy/surface/default.asp.
Taiwan Assassin. 2004. Retrieved on April 7, 2008, from http://www.tzengs.com/News/Assasin/photos_.htm.
Talmadge, Caitlin. 2008. Closing Time: Assessing the Iranian Threat to the Strait of Hormuz. Retrieved on August 2, 2008, from http://belfercenter.ksg.harvard.edu/publication/18409/closing_time.html.
Tellis, Ashley. 2007. China's Military Space Strategy. Retrieved on January 28, 2008, from http://www.informaworld.com/smpp/section?content=a780978527&fulltext=713240928.
Thai Truckers Join Global Fuel Price Protest. 2008. Retrieved on August 1, 2008, from http://business.smh.com.au/business/thai-truckers-join-global-fuel-price-protest-20080611-2oy3.html.
The Christian Science Monitor. 2006. China's new shopping craze: 'team buying'. Retrieved on August 1, 2008, from http://articles.moneycentral.msn.com/SavingandDebt/FindDealsOnline/ChinasNewShoppingCrazeTeamBuying.aspx.
The Cyber Raiders Hitting Estonia. 2007. Retrieved on February 12, 2008, from http://news.bbc.co.uk/2/hi/europe/6665195.stm.
The Passion of Anonymous. 2008. Retrieved on July 14, 2008, from http://www.newsweek.com/id/109410.
Thornburgh, Nathan. 2005. Inside the Chinese Hack Attack. Retrieved on July 21, 2008, from http://www.time.com/time/nation/article/0,8599,1098371,00.html.
Thornburgh, Nathan. 2005. The Invasion of the Chinese Cyberspies. Retrieved on March 2, 2008 from http://www.time.com/time/magazine/article/0,9171,1098961,00.html.
Tkacik, John J Jr. 2007. Trojan Dragons: China's Cyber Threat. Retrieved on March 20, 2008, from http://www.heritage.org/Research/asiaandthepacific/bg2106.cfm.
Towards one laptop per child. 2006. Retrieved on July 28, 2008, from http://www.sunstar.com.ph/static/ceb/2006/07/24/bus/towards.one.laptop.per.child.html.
Trahan, Jason. 2008. Teen wouldn't quit his hacking ways, FBI says. Retrieved on August 31, 2008, from http://www.dallasnews.com/sharedcontent/dws/news/nation/stories/DN-swating_31met.ART0.West.Edition1.4ddc7cf.html.



Published by ePublications@bond, 2008

Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80 Copyright © 2008 Jason Fritz

United States General Accounting Office (GAO), Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures, Statement of Keith A. Rhodes, Chief Technologist, August 29, 2001 (GAO-01-1073T), see http://www.gao.gov/new.items/d011073t.pdf

Use of Social Network Websites in Investigations. 2008. Retrieved on August 12, 2008, from http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations.

Vallance, Chris. 2008. US Seeks Terrorists In The Web Worlds. Retrieved on March 8, 2008, from http://news.bbc.co.uk/2/hi/technology/7274377.stm.

Vamosi, Robert. 2008. Anonymous posts another video against Scientology. Retrived on July 14, 2008, from http://news.cnet.com/8301-10789_3-9859513-57.html.

VoIPWiki Blog. 2006. Skype Protocol Has Been Cracked. Retrieved on July 14, 2008, from http://www.voipwiki.com/blog/?p=16.

Wagstaff, Jeremy. 2005. The First U.S.- China Cyberwar. Retrieved on July 27, 2008, from http://loosewire.typepad.com/blog/2005/12/the_first_uschi.html.

Warrick, Joby and Johnson, Carrie. 2008. Chinese Spy Slept In US For 2 Decades. Retrieved on April 3, 2008, from http://www.washingtonpost.com/wp-dyn/content/story/2008/04/02/ST2008040204050.html.

Warren, Peter. 2006. Smash and grab, the hi-tech way. Retrieved on July 18, 2008, from http://technology.guardian.co.uk/weekly/story/0,,1689093,00.html.

Waterman, Shaun. 2008. Analysis DHS Stages Cyberwar Exercise. Retrieved on April 10, 2008, from http://www.spacewar.com/reports/Analysis_DHS_stages_cyberwar_exercise_999.html.

Waterman, Shaun. 2008. Analysis: Russia-Georgia Cyber War Doubted. Retrieved on August 18, 2008, from http://www.spacewar.com/reports/Analysis_Russia-Georgia_cyber war_doubted_999.html.

Waterman, Shaun. 2008. Chinese Cyberattacks Target US Think Tanks. Retrieved on March 8, 2008, from http://www.spacewar.com/reports/Chinese_Cyberattacks_Target_US_Think_Tanks_999.html.

Waterman, Shaun. 2007. China Has .75 Million Zombie Computers In US. Retrieved on March 17, 2008, from http://www.upi.com/International_Security/Emerging_Threats/Briefing/2007/09/17/china_has_75m_zombie_computers_in_us/7394/.

Waterman, Shaun. 2007. Who cyber smacked Estonia? Retrieved on January 17, 2008 from http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

Wayner, Peter. 1999. Hacker Attacks on Military Networks May Be Closer to Espionage. Retrieved on August 10, 2008, from http://www.landfield.com/isn/mail-archive/1999/Mar/0022.html.

Weber, Harry. 2008. FAA Says Communications Breakdown Delaying Flights. Retrieved on August 28, 2008, from http://news.yahoo.com/s/ap/20080826/ap_on_re_us/faa_communication_breakdown;_ylt=A0WTUeXUlbRISucAawSs0NUE.

Weber, Tim. 2007. Criminals may overwhelm the web. Retrieved on August 1, 2008, from http://news.bbc.co.uk/1/hi/business/6298641.stm.

Wei, Michael. 2008. Facebook Targets China, World's Biggest Web Market. Retrieved on June 20, 2008, from http://www.reuters.com/article/ousiv/idUSSHA17883120080620.

Wensheng, Wang. 2006. Bridging the Digital Divide Inside China. Retrieved on July 28, 2008, from http://zoushoku.narc.affrc.go.jp/ADR/AFITA/afita/afita-conf/2002/part7/p533.pdf.

WFTV. 2008. Girls Record Brutal Attack On Teen To Allegedly Post on YouTube. Retrieved On May 10, 2008, from http://www.wftv.com/news/15817394/detail.html.

Winkler, Ira. 2005. Guard Against Titan Rain Hackers. Retrieved on January 8, 2008, from http://www.computerworld.com/securitytopics/security/story/0,10801,105585,00.html.

Winkler, Ira. 2007. How To Take Down The Power Grid. Retrieved on June 7, 2008, from http://www.internetevolution.com/author.asp?section_id=515&doc_id=136047.

Winkler, Tim. 2003. Dragonflies Prove Clever Predators. Retrieved on February 10, 2008, from http://info.anu.edu.au/ovc/media/Media_Releases/_2003/_030605Dragonflies.asp.

Winn, Patrick. 2008. Hypothetical attack on U.S. outlined by China. Retrieved on February 23, 2008, from http://www.airforcetimes.com/news/2008/01/airforce_china_strategy_080121/.

Whitney, Mike. 2008. Three Internet Cables Slashed In A Week. Retrieved on July 4, 2008,

*Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80* *Copyright © 2008 Jason Fritz*

from http://www.globalresearch.ca/index.php?context=va&aid=7987.
World Wide Military Expenditures. 2007. Retrieved on August 12, 2008, from http://www.globalsecurity.org/military/world/spending.htm.
Wortzel, Larry M. 2007. China's Nuclear Forces: Operations, Training, Doctrine, Command, Control, and Campaign Planning. US Strategic Studies Institute. Retrieved on December 11, 2007, from www.StategicStudiesInstitute.army.mil/.
Yahoo Implicated In Third Cyberdissident Trial. 2006. Retrieved on March 11, 2008, from http://www.rsf.org/article.php3?id_article=17180.
Yeates, Ed. 2007. Exoskeleton Turns Humans Into Terminators. Retrieved on March 10, 2008, from http://www.youtube.com/watch?v=h2jlIRKswnQ.
Yue, Qi and Yue Qin. 2008. China Regime Implicated In Staging Violence In Tibetan Protest. Retrieved on April 3, 2008, from http://chinaview.wordpress.com/2008/03/29/photo-china-regime-implicated-in-staging-violence-in-tibet-protest/.
Zheng, Yongnian and Sow Keat Tok. 2007. 'Harmonious Society' and 'Harmonious World': China's Policy Discourse under Hu Jintao. Briefing Series, Issue 26, October. China Policy Institute. Retrieved on October 2, 2008, from http://www.nottingham.ac.uk/shared/shared_cpi/documents/policy_papers/Briefing_26_Harmonious_Society_and_Harmonious_World.pdf.