Reuters RTXP5C5 by Nir Elias

People's Liberation Army (PLA) tanks rumble through Tiananmen Square in Beijing to mark the 60th anniversary of the founding of the People's Republic of China, 1 October 2009.

# The Past, Present and Future of Chinese Cyber Operations

**by Jonathan Racicot**

Captain Jonathan Racicot *is currently posted to the Canadian Forces Intelligence Command, and he has been following events in the cyber environment for years. He obtained his bachelor degree in Computer Science from the University of Montreal in 2006, and then joined the Canadian Armed Forces in 2007 as a Signals Officer. He currently specializes in keeping track of Advanced Persistent Threats, as well as pursuing additional research on Computer Security and Computer Network Operations in his free time.*

## Introduction

An unprecedented flurry of intelligence reports by private security firms are homing in on the cyber domain, seizing the opportunity to illuminate cyberspace as an emerging priority for defence interests. Cyberspace, as the fifth battlespace, however, is not new. What makes cybersecurity particularly challenging in a modern context is that it is often misunderstood and prone to sensationalism.

China, as one of many alleged actors on the frontier of cyber espionage, is best understood by briefly examining the past century, how it influences contemporary cyber operations attributed to Chinese-based actors, and how they could be used against the CAF in a potential Southeast Asian conflict.

On 29 March 2009, *The New York Times* reported that a wide-scale espionage network had been discovered by researchers from two Canadian cybersecurity entities: the SecDev Group and Citizen Lab at the University of Toronto.[1] Labeling it the GhostNet, researchers had shed light on a network of 1295 compromised computers in 103 countries. Most of the infected machines were located in the office of the Dalai Lama, and in economic and diplomatic offices for various Southeast Asian governments.[2] Although not the first alleged Chinese cyber espionage campaign to be reported, GhostNet was one of the largest and most intrusive espionage networks known at the time. Within this environment, Chinese actors are the most active and persistent in conducting cyber espionage for economic purposes. Along with Russian actors,[3] they cost the US economy up to $USD 300 billion a year.[4]

## The Past

Even in this day and age, the First Opium War of 1839, which pitted the British and Chinese empires against each other, still represents the key event of modern China, the event

© National Maritime Museum, Greenwich, London.

The technologically-superior iron steam ship *Nemesis* of the East Indian Company destroying Chinese war junks in Anson's Bay, 7 January 1841.

which marked the beginning of its "Century of Humiliation," and modeled Chinese interaction with the West for years to come. Under the rule of the Qing dynasty, the empire was compelled, not just once, but twice into agreeing to the terms of the "unequal treaties," which would cede control of Hong Kong to Britain and force the opening of additional ports for trade, including the ravaging commerce of opium.[5] Despite outrageous and optimistic claims of imminent victory in their correspondence with the emperor, the Qing officials knew very well that British ships and cannons were far superior to their own, that they were also hampered by an ad-hoc, undisciplined military,[6] and defended by decaying fortresses.[7] Additionally, accustomed to fighting pirates off the coast, they lacked any 'blue sea' war fighting capability.[8] In other words, the Chinese were facing an adversary with a superior technology. This was further reinforced with the arrival of the *Nemesis*, the first all-iron ocean ship, whose destructive power during an encounter in Chuenpee astonished the Chinese, who fled their junks with shock and awe.[9]

By the end of the Second Opium War in 1860, Qing China had learned the harsh consequences of complaisance. So convinced of the superiority of Chinese civilization compared to the one of the "foreign barbarians,"[10] it had isolated itself and failed to establish scientific and technical exchanges with the rest of the world, thus creating a technology lapse for which they paid dearly.

During the same period, neighboring Japan was stunned by the arrival of the large modern warships of American Commodore Matthew C. Perry. Seeing the looming threat of Western colonial powers, the Meiji Emperor of Japan quickly decided to modernize, integrating Western technologies, and political and economic systems within their own society. Known as the Meiji Restoration, Japan went from a feudal society to an industrial society between 1868 and 1912, modernizing every aspect of its society, including its military. This aggressive modernization would prove highly successful for the Japanese. In 1895, their Imperial Army would force the Qing Dynasty to sign the Treaty of Shimonoseki. This treaty and its contents would have a profound effect upon the Chinese population. For two millennia, China had visualized itself as the universal empire, to which all uncivilized non-Chinese neighbors owed tribute to the Son of Heaven, i.e., the Chinese Emperor.[11] As such, Japan, seen as a cultural tributary by the Chinese, would shock the population even more than the British insult of 1860, which later resulted in the Boxer Rebellion. Amongst others, the Japanese victory was credited to the modernization and aggressive industrialization achieved by adopting Western ideas and technology.[12] These reforms would also pay off in the unexpected Japanese victory in the Russo-Japanese War of 1904 and the Japanese invasion of Manchuria in 1937. Chinese defeats by external threats were caused by numerous factors, but a key determinant was the superior technological and logistical capability of foreign military forces.

The Granger Collection, NYC, #0060527

Commodore Matthew Perry, USN

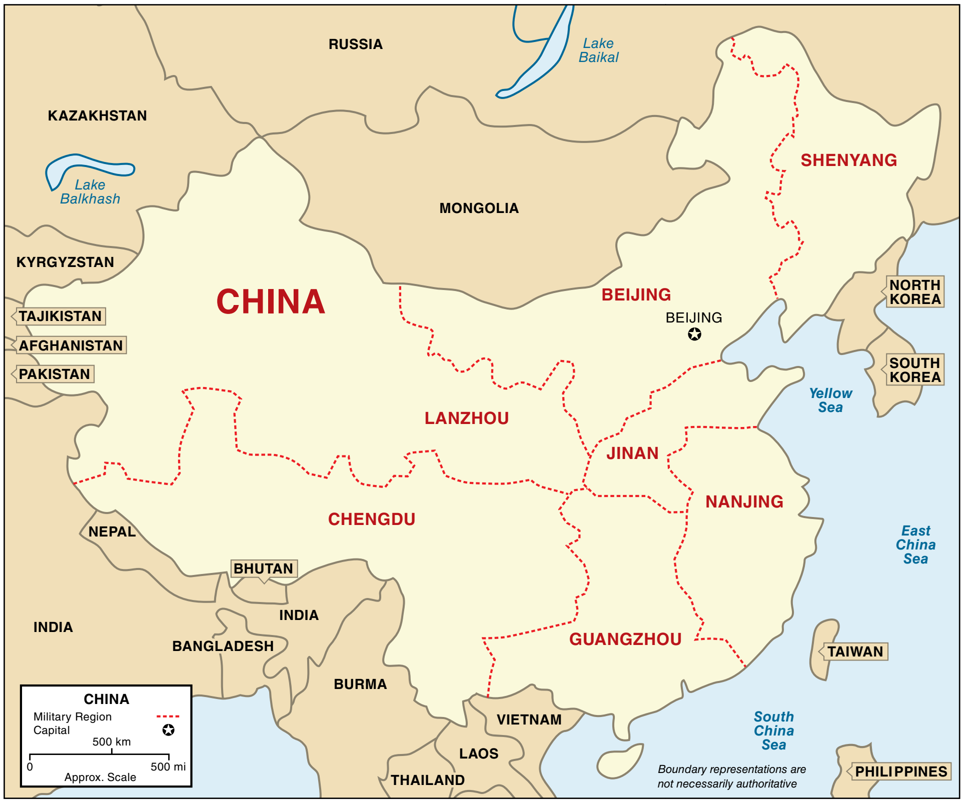
Following the devastating effects of the Second World War, Mao's Cultural Revolution did nothing to improve the rate of modernization of Chinese society. However, it introduced a concept that would influence modern Chinese military thinkers with regard to the development of information warfare: the People's War. Although originally defined by Mao as a way to entrap Nationalist troops, the concepts of using the masses, inferior technology to subdue technologically superior adversaries, and the involvement of the entire society in conflicts,[13] would be found compatible with the development of information warfare. When Deng inherited the head of the People's Republic of China, the country was on its way to collapse. 34 percent of the population had nothing more than a primary education, 28 percent were illiterate or semi-illiterate, and a mere 0.87 percent had acquired a college education.[14] Estimating that China lagged 20 years behind the developed countries, it came as no surprise that Deng passionately called for the modernization of Chinese society, based upon the Meiji Restoration:[15]

> *The key to achieving modernization is the development of science and technology. And unless we pay special attention to education, it will be impossible to develop science and technology. [...]As early as the Meiji Restoration, the Japanese began to expend a great deal of effort on science, technology and education. The Meiji Restoration was a kind of modernization drive undertaken by the emerging Japanese bourgeoisie. [...] In the army as well, it is necessary to encourage scientific research and education at the same time. Without knowledge of modern warfare, how can we fight a modern war? Leading army cadres should become knowledgeable and respect knowledge. We should establish schools at various levels to enable leading army cadres to master modern science, culture and modern warfare in the course of training.*

In 1978, a year after the preceding speech, 433 Chinese students would be sent to study in the United States. Various disciplines, such as physics, radio-electronics, computer science, and engineering were identified as the top four programs, accounting for 35 percent of the delegation.[16] In 1986, Deng launched the 863 and Super 863 programs, major efforts to accelerate the legal and illegal acquisition of technologies, including strategic military technologies such as laser, information technology (IT), dual-use technologies, and energy.[17] The push from Deng, chair of the Central Military Committee (CMC), to modernize echoed into the People's Liberation Army (PLA) and primarily affected the PLA Navy (PLAN) and PLA Air Force (PLAAF).[18] On an interesting note, back in the 1980s and 1990s, it was estimated that the PLA had interests in between 10,000 and 50,000 state-owned industries[19] responsible for both civilian and military production, while providing a significant source of revenue and thus creating a major military-industrial complex. The reforms to transfer ownership of these companies from the PLA to commercial entities eventually spanned private industries founded by ex-military members, Huawei Technologies Company Limited being a pre-eminent example.[20] By the end of 1998, it was estimated that approximately 2000 to 3000 enterprises remained linked to the PLA.[21] It is, however, very likely that strong relationships between the PLA and the industry at large remain as the concept of People's War and "Unrestricted Warfare," are believed to be alive and prospering nowadays. While the People's War defined war as a struggle between nations rather than militaries, "Unrestricted Warfare" defines the utilization of every aspect of society, such as the economy, communications, industry, diplomacy, and so on, to be required in a conflict with a stronger power.[22] The concept also emphasizes "Network Warfare," which proposes the idea of attacking the critical infrastructure of a superior adversary to cripple its economy, industry, and communications.

It is therefore not surprising that the concepts of a 'high-tech war' and of 'information warfare' provoked interest within the senior leadership of the PLA. As the Gulf War raged on and then the Bosnian conflicts emerged, so did the concept of Network Centric Warfare. Rightfully or not, the PLA were convinced that the Americans used computer viruses and network attacks against the Iraqis' networks, and they viewed it as a confirmation of the importance of developing information warfare capabilities.[23] As weapon systems and command and control networks were being "informationized" – the Chinese concept for Network-Centric Warfare – networks represented for the PLA's 'brass' the *Shashou Jian* (Assassin's Mace), that is, the capacity to deal a decisive blow to a superior enemy using inferior weapons, in line with Mao's concept of the People's War.[24]

If the past is any indication of the present, and it usually is, China has learned the pitfalls of being technologically inferior to its neighbors. Within a century, its own fall from being the Celestial Empire to a third world country at the hands of foreign powers is not forgotten. Using concepts from the People's War and the reforms already underway, China is now using cyber operations to modernize its society by acquiring intellectual property and other relevant intelligence with the goal of obtaining information dominance.



Shutterstock 98865608, redrawn by Accurate

China and its military regions

## The Present

At the beginning of the millennium, the dialogue with respect to about information warfare appeared abundantly in the PLA's literature,[25,26] and information warfare was most certainly taken seriously at higher levels. As of 2011, it was estimated that the PLA had integrated multiple technical reconnaissance bureaus (TRB) across the various elements of the PLA, including the PLAN and the PLAAF. The 3rd Department (3PLA), responsible for SIGINT, is believed to host a total force of 130,000 members, working in 12 TRBs and three research institutes.[27] According to the Project 2049 Institute, the roles and responsibilities of these 12 TRBs are as follows:[28]

- 1st TRB (Unit 61786), located in Beijing and overseeing 12 offices across China, is believed to be involved in cryptography, and is the only military organization involved in the 863 program. It also maintains close ties with the Sichuan University's Information Security and Network Attack and Defense Laboratory, as well as hosting the 57th Research Institute and the Chengdu Military Region 1st TRB.
- 2nd TRB (Unit 61398) is believed to be mostly interested in targeting technological, scientific, economic, and commercial and military intelligence elements in the English-speaking countries, including the United States and Canada. It is worthwhile mentioning that Unit 61398 was exposed in February 2013 by *Mandiant*,[29] wherein it was reported that the unit may have compromised up to 141 companies spanning 20 major industries, using well-defined standard operating procedures (SOPs) to 'steal' a large amount of intellectual property. On average, cyber operators from the 2nd TRB were able to maintain access to networks for a full year, with the longest compromise lasting four years without being detected. The span of their command and control infrastructure encompassed between 850 and 1000 machines located in 13 countries.
- 3rd TRB (Unit 61785) seems to focus upon wireless communications. It would also appear that members of the Third Division have carried out joint studies with Shanghai Jiaotong University's Department of Computer Science and Engineering, and have conducted research on cyber warfare and vulnerability assessments in Android devices.[30]
- 4th TRB (Unit 61419) is concerned with targets in Japan and Korea, and possibly other South Asian countries.
- 5th TRB (Unit 61565) maintains multiple parabolic dishes on its rooftop, and is assessed as collecting against Russia.
- 6th TRB (Unit 61726) may be interested in Taiwan and Southeast Asian nations, such as Thailand, Vietnam, and Singapore.
- 7th TRB (Unit 61580) may be involved in research with regard to computer network attacks (CNA) and computer network defence (CND).
- 8th TRB (Unit 61046) employs linguists knowledgeable with respect to languages spoken in Europe, the Middle East, and Latin America. It is possible that the 8th TRB is involved in Africa as well.
- The 9th TRB may be the strategic intelligence TRB, as well as having responsibility for maintaining the databases needed by other TRBs.
- 10th TRB (Unit 61886) is believed to be invested with the Central Asian or Russian mission, possibly focusing upon telemetry and missile tracking and/or nuclear testing.
- 11th TRB (Unit 61672) may be related to Russia. It is unknown in what way the mission of the 11th TRB would differ from the mission of the 5th TRB.
- 12th TRB (Unit 61486) seems to be related to SIGINT and space technologies, including satellites and interception of satellite communications.

Additionally, each of the seven Military Regions (MR) oversees their own TRBs with guidance from the 3PLA. From the initial twelve military regions in 1954, the number was reduced to seven by 1988. Hence, some regions now have two TRBs:

- Beijing Military Region (Unit 66407): This TRB may have a mission revolving around Russia and Mongolia.

- Chengdu Military Region (Units 78006 and 78020): this TRB is suspected of being involved in computer network exploitation (CNE) operations, and may target English-speaking countries. Given its location, it is probable that it is involved in Southeastern Asian countries as well.
- Guangzhou Military Region (Unit 75770): probably involved in cyber operations as well as being noted for studying viruses and malware, in addition to working on Internet telephony surveillance.
- Jinan Military Region (Unit 72959): has been reported as employing 670 technical specialists as well as Korean, Japanese, and English linguists, possibly indicating a focus on countries within the Pacific area.
- Lanzhou Military Region (Units 68002 and 69010): oversees two TRBs, one of which may play a key role in SIGINT, and it has offices located around Central Asia.
- Nanjing Military Region (Units 73610 and 73630): the Nanjing TRBs may focus their interests toward Taiwan and the United States.
- Shenyang Military Region (Unit 65016): appears to target Russia, Korea and Japan.

Both the Navy and Air Force elements have their own TRBs, as does the Second Artillery. The PLAAF is believed to host three TRBs:

- 1st TRB (Unit 95830) manages an underground network operation centre, as well as a network of direction finding sites for air defence in eastern and northeastern China.
- The 2nd TRB oversees a network of collection and direction finding sites along the coast in Fujian and Guangdong. Presumably, their mission consists of the monitoring of Taiwan's Air Force (ROCAF) communications networks.
- Finally, the 3rd TRB most likely monitors air activity and air defence communication networks along China‘s southwestern, western, and northwestern borders.

For its part, the PLAN is known to oversee two TRBs, one headquartered in Beijing under the Unit designator 91746. Since the PLAN operates three fleets (North Sea, East Sea, and South Sea), it may not be farfetched to believe a 3rd TRB exists, but this is unconfirmed at this time.

Although not identified within the report, some or all of the PLAN and PLAAF TRB are likely involved in cyber operations, focusing upon acquiring intellectual property, and military and diplomatic intelligence related to their particular element. This assumption is reinforced by the priority placed upon modernizing the navy and the air force.

4PLA is also researching and developing computer network attack (CNA) techniques, tactics, and procedures (TTPs). It maintains oversight of the PLA Electronic Engineering Academy, as well as the 54th Research Institute, which, in turn, has ties with industry.

Other government and commercial entities are also taking part in CNE operations. The Ministry of State Security (MSS), the foreign intelligence agency of the PRC, is very likely a potential source of cyber operations with mandates other than the PLA. Some of their resources are likely focused upon monitoring the "five poisons," which include the Uyghurs, Tibetans, Falun Gong followers, democracy advocates, and promoters of an independent Taiwan.[31] The need for modernization has also inspired a new industry of private security contractors which will conduct cyber operations, develop weapons, or run an intelligence-for-profit model.[32] All these organizations are recruiting students who have gone through a Ministry of Education program that teaches both defensive and offensive operations such as 'spear-phishing,' – targeted e-mails containing a disguised malicious attachment or link – malware, attacks against web servers, and password cracking.[33] The effort to use information technology as the main impetus toward modernization has involved practically all components of Chinese society.

| Estimated Starting Year of Suspected China Major Cyber Espionage Operations | | | |
|---|---|---|---|
| **Actor/Operation** | **Year** | **Targeted Countries, Regions** | **Targeted Sectors** |
| **Nortel** | 2000 | Canada | Information Technology |
| **Titan Rain[36]** | 2002 | United States | Defense, Space |
| **Net Traveler[37]** | 2004 | Mongolia, Russia, India | Diplomacy, Government |
| **APT1[38]** | 2006 | United States | Information Technology, Aerospace, Government |
| **Gh0st** | 2007 | Vietnam, United States, China | Diplomacy, Government, NGO |
| **Operation Aurora[39]** | 2009 | United States | Information Technology, Defense |
| **Elderwood[40]** | 2009 | United States, Canada | Defense, Shipping, Aeronautics |
| **Night Dragon[41]** | 2009 | United States, Kazakhstan, Taiwan | Energy |
| **Ke3chang[42]** | 2010 | Europe, G20 | Diplomacy, Aerospace, Defense, Energy, Government |
| **Government of Canada[43]** | 2011 | Canada | Government, Defense |
| **Nitro[44]** | 2011 | United States, Bangladesh, U.K | Chemical |
| **Hidden Lynx[45]** | 2011 | United States, Taiwan | Finance, Education, Government |
| **Icefog[46]** | 2011 | South Korea, Japan | N/A |

Table 1 – List of major cyber operations attributed to China-based threat actors, including estimated started year, top targeted countries and most frequently targeted sectors.

**Estimated Cost of Conducting a 12-month Spear-Phishing Campaign by a Section ($USD)**

| Category | Item | Quantity | Low | High | Average |
|---|---|---|---|---|---|
| Personnel | Officers | 1 | 6,000 | 10,800 | 8,400 |
| | Enlisted | 5 | 9,600 | 24,000 | 16,800 |
| Infrastructure | Domains | 12 | 0 | 191.88 | 95.94 |
| | Server | 1 | 0 | 599.88 | 299.94 |
| | Network | 1 | 0 | 39.99 | 19.995 |
| | Internet Connectivity | 1 | 120 | 240 | 180 |
| Tools and Weapons | Zero-day Exploit | 1 | 50,000 | 100,000 | 75,000 |
| | Remote Access Tool | 1 | 0 | 120,000 | 60,000 |
| Hardware | Workstations | 6 | 1,200 | 7,200 | 4,200 |
| Total | | | 66,920 | 263,072 | 164,996 |

Table 2 - Estimated cost of a 12-months spear-phishing campaign using a zero-day exploit by a CNO section.

## Operations

Given the requirement from the highest political circle to modernize, combined with the imposing military structure built for information warfare, it comes as no surprise that the bulk of cyber operations conducted by the Chinese nowadays are actually cyber espionage missions, mostly against defence industries, but also aimed at economic and political targets. The earliest known Canadian compromise dates from 2000, at which time Chinese hackers were believed to have infiltrated the networks of Nortel. The compromise persisted until the bankruptcy of Nortel in 2009, and it is widely believed to be a major cause of the demise of the company.[34] This breach was also the first in a long line of cyber espionage operations that are ongoing today.[35]

Table 1 chronicles the events of importance which have been linked to China. Other events less reported have also surfaced, such as the compromise of Canadian energy company Telvent,[47] and many others targeting Taiwan.[48]

Attribution of offensive cyber operations remains problematic in this battlespace, as CNE operators often utilize intermediate attack points to obfuscate their origin. For attacks that link back to China, it is possible that computers located in China were used as proxies. This plausible deniability makes cyber operations low risk compared to other forms of espionage, and it explains why cyberspace is increasingly used as a means to collect valuable information by governments.

> **"Attribution of offensive cyber operations remains problematic in this battlespace, as CNE operators often utilize intermediate attack points to obfuscate their origin."**

Another complication for assigning attribution with confidence is that the location of a detected compromise is based upon the Internet Protocol Address (IP) of the machine – a number used to identify machines on the Internet; somewhat similar to a postal address – contacting the command and control server. The target may actually be owned by another country. For example, in many cases, targets in China are actually embassies of foreign countries, rather than Chinese-owned assets. Also, some of the items listed in Table 1 are *named operations* versus *named actors*, and cannot be linked to a physical unit solely on their target.

Finally, attribution may be difficult, since Chinese cyber espionage tactics are becoming well-known. As a consequence, criminal actors and other nation states may use similar techniques that give the false impression that an attack originated from China. The adversary's motivation is recognized as a hallmark of the intelligence function, whereby attribution can be unmasked by recognizing patterns and a known need to fulfill specific intelligence gaps that are consistent with long-term political and economic goals.

All the operations noted above used 'spear-phishing' as their preferred delivery method. This technique has been used successfully for the past few years, since it exploits the weakest link of networks: the users. Additionally, given its low cost and the value of the data stolen, this TTP likely provides an excellent return on investment. A single spear-phishing operation roughly costs between $CAD71,211.00 and $CAD279,944.00 per year, depending upon the sophistication of the operation. In Table 2, we have included a simple estimate of a 12-month spear-phishing campaign by a single adversarial section. The lowest cost includes the usage of free services and Remote Access Tools (RATs). For the highest cost, we assume the usage of civilian commercial services and criminal services. In both cases, we include the cost of one zero-day exploit – an unknown vulnerability in applications that lead to compromise – for Microsoft Office. Note that adversaries do not always use zero-day exploits, and this decreases the cost of the campaign even further.

The PLA does not disclose the pay scale of its members. Based upon open source reporting,[49] we approximated the salaries, but can safely assume that they are lower than the salaries of equivalent ranks in the CAF. Many of the required tools and weapons, such as the *Poison Ivy* RAT, are freely available on the Internet. Other weapons, such as the *Cool Exploit* kit, can cost up to $USD 10,000.00/month. Zero-day exploits are the most expensive

Reuters RTXP5E9 by China Daily Information Corporation [CDIC]

Tracked carriage motor howitzers take part in a military parade in central Beijing.

items, and costs vary from $USD 5000.00 to $USD 250,000.00, depending upon the vulnerable system.[50] On average, a zero-day exploit can last for 312 days,[51] before being patched and rendered useless to an adversary.

Yet, using these simple, low cost TTPs, an adversary can steal intellectual property valued at millions, and can severely damage the economy of a home country. Additionally, the theft of military technologies greatly reduces the technological advantage of modern militaries, an aspect that China likely remembers clearly and does not wish to be reproduced in the future if it wishes to assert regional dominance.

> **"Although cyber espionage is certainly a priority for China, it doesn't discount other possible targets."**

One indirect consequence of these activities is that it forces corporations, as well as government departments, to implement costly cyber defences. Calculating the costs of defending a network is tricky. While equipment can last for multiple years, it requires annual maintenance and support contracts. Based upon the pay scale of the Canadian Armed Forces, a section of one captain and five corporals at the lowest level of pay, estimated collectively at $CAD357, 264.00,[52] would still be more expensive than a year-long spear-phishing campaign. The Canadian Forces Network Operations Centre (CFNOC) spent approximately $CAD1,120,000.00 during fiscal year 2012-2013 for surveillance activities of CAF networks. In cyber operations, as in most kinetic operations, the advantage is owned by the attacker.

Although cyber espionage is certainly a priority for China, it does not discount other possible targets. These include Supervisory Control and Data Acquisition Systems (SCADA), systems managing critical infrastructure, such as water pumps, thermal plants, electric grid, and so on. A *Trend Micro* analysis observed activity against a decoy water pump system between 2012 and 2013. The results indicated that 58 percent of the attacks came from Russia. However, 56 percent of the critical attacks against the decoy originated from within China.[53] In one instance, tactics similar to the one used by APT1 were observed. Sensitive files were exfiltrated, and access was maintained periodically, but no action was taken on the decoy water pump. This single instance is far from being sufficient to indicate a trend. However, should China want to gain an advantage on a superior adversary, it would likely seek to disrupt critical infrastructure and communications as a 'first strike' approach to gain information dominance.[54] PLA elements would therefore seek to gain and maintain persistent access to these systems until a disruption/denial operation is needed.

Given the low cost and low risk of conducting cyber operations versus the high cost of cyber defences and the supporting bureaucracy, one can safely assume that Chinese cyber espionage will continue until either one of these conditions is fulfilled:

1) the cost of conducting cyber operations will be greater than the cost for defences;

AFP photo XXJPBEE001076_20111115_TPPFN1A001

2) the risk of conducting cyber operations will be too high; or

3) China attains a close scientific, technological and military parity with the West.

## The Future

Given the low cost of manufacturing IT equipment in China, and the low wages of PLA members, costs of cyber operations are likely to remain low versus costs for defences. Additionally, as demand for network defences increases, Western companies are very unlikely to reduce the price of their solutions. As for risk, since attribution is difficult, especially for companies, little-to-no international law on cyber warfare exists and the benefits are high, the risk will remain relatively low for at least the next three-to-five years. Finally, China remains unable to match the United States military despite rapid Chinese modernization. However, should a regional conflict such as a territorial dispute with neighboring countries emerge, it may become tempting to leverage computer network attacks (CNA) as force projection.

The PLA sees computer network operations (CNO) as first-strike operations in order to seize 'information dominance' to disrupt critical infrastructure and C4ISR systems. As such, as of 2005, the PLA has integrated both *cyber defensive* and *cyber offensive* operations to achieve information dominance in their military exercises.[55] In 2013, the Chinese Ministry of National Defense reiterated their usage of information systems as a main enabler in order to win local wars;

> *China's armed forces firmly base their military preparedness on winning local wars under the conditions of informationization, make overall and coordinated plans to promote military preparedness in all strategic directions, intensify the joint employment of different services and arms, and enhance warfighting capabilities based on information systems.*[56]

Based upon this information, we can assume that until China considers itself to be competitive with the US military, it will focus upon winning local wars. At the moment, China is embroiled in multiple territorial and sovereignty conflicts within the South China Sea, such as the Senkaku/Diaoyu islands with Japan, and the Spratleys Islands with the Philippines. It also maintains its assertion over Taiwan, which it considers to be part of Chinese territory. Many of these conflicts have escalated in the past year, especially with Japan, as China decided to unilaterally include the islands into their Air Defense Identification Zone.[57] In fact, China already produced a video game simulation of the PLA's 'retaking' of the Senkaku/Diaoyu Islands from Japan.[58] Therefore, the world could witness the usage of Chinese computer network attacks in a regional conflict to claim territory.

How could China use CNA to achieve its goal in a local war, given that most of its neighbors have defence treaties with the United States? One of the scenarios detailed by Chinese intelligence

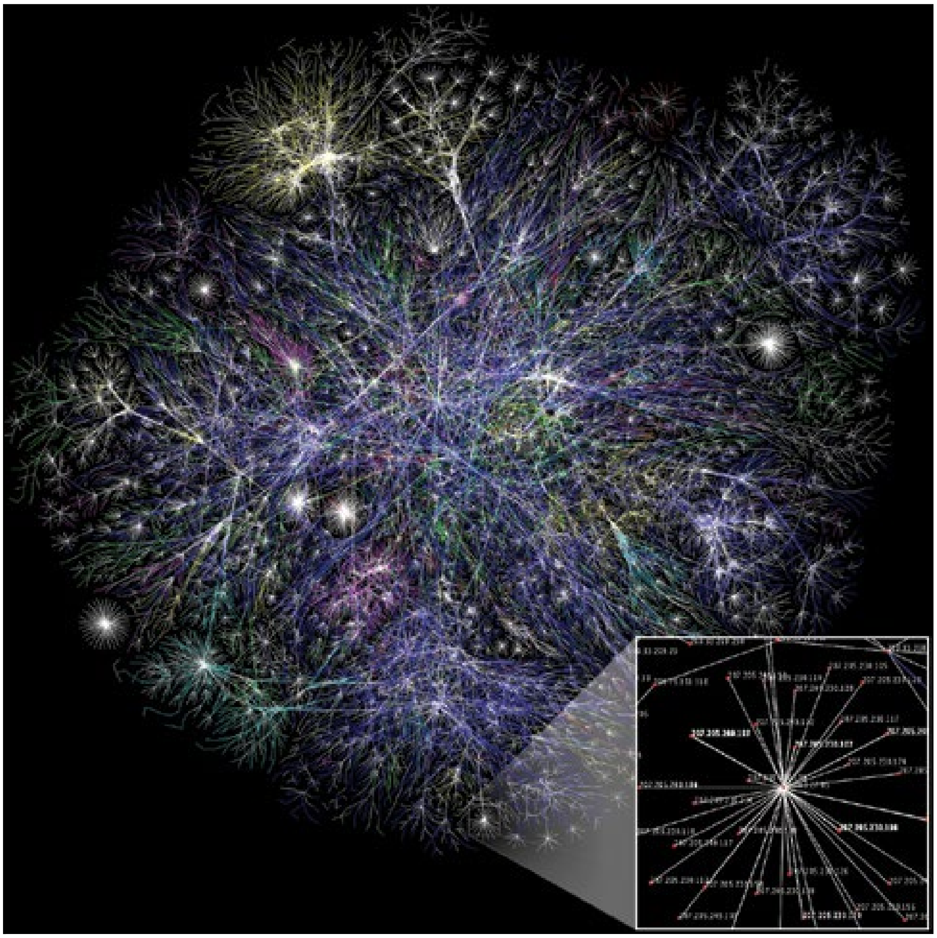
IMAGINECHINA AFP PAU324481_02

capabilities expert Dr. James Mulvenon hypothesizes China invading Taiwan and utilizing computer network attacks for delay operations, while US reinforcements are in their mobilizing and deployment phases.[59] Such a computer network attack would be directed against unclassified, logistical networks which offer a much easier target than closed operational networks. Compromise of logistical networks is within the capabilities of PLA information warfare units using the current TTPs, even within the reach of organized cyber criminals. Since the disruption of these networks would have to occur in early phases of a conflict, peacetime CNO will focus upon gaining and maintaining access to these networks without being detected.

Within the Canadian Armed Forces, the Defence Wide Area Network (DWAN) is the primary logistical network. With over 120,000 DWAN accounts, the department relies heavily upon DWAN for day-to-day activities. It hosts capabilities often dismissed as administrative, but that would cause major disruptions in CAF operations, should they become unavailable. Among them is the Defence Resource Management Information System (DRMIS), which includes the Material Acquisition and Support Information System (MASIS) used for maintenance, supplies from defence contractors, corporate operations, and support to military operations.[60] Disrupting DRMIS to delay or prevent West coast warships or air assets to support a US intervention in the Pacific could be possible. Another possibility would be to infect the DWAN with a "wiper" worm, which, once on the network and activated, would erase all data on all infected machines and render them unserviceable. Such a tactic was used against Saudi Aramco,[61] and on South Korean media and banks.[62] If critical elements of the network become infected, it could render the entire DWAN unusable, including mobile devices, e-mails, and logistics systems onboard ships. Given the current techniques observed, using CNO to delay or disrupt a military intervention in the Pacific is a plausible scenario.

This strategy will, however, require PLA elements to act quickly and to use their 'Assassin's Mace' against an adversary. As such, they would also need, solely from an information warfare angle, to gain information dominance by taking over or disrupting the adversary's communications systems. This would make telecommunications companies a target, as well as networks of critical infrastructure or governmental organizations. These tactics were used during the Georgian conflict of 2008. Again, exploitation of these networks would occur during peacetime, and those networks attack plans would be activated during a conflict. The skills required for computer network attacks are very similar to the skills currently needed for CNE. Such networks would be disrupted prior to a kinetic operation against the adversary in order to use the confusion to its advantage and follow the 'first strike' doctrine.

In Canada, the protection of critical infrastructure is still nascent as Public Safety attempts to establish links with industry, which usually does not report incidents, or dismisses them as technical problems. The extent to which the critical infrastructure is vulnerable is hard to assess, since the scrutiny of it is virtually nonexistent. SCADA systems are often the networks causing alarmist statements, given the lethal consequences they could possess. As



Wikimedia Google.com/file/d/0BaEq2dBpNcWEtelZKUENsSIU

Partial map of the Internet from 2005, which contains less than 30 percent of the Class C addresses. Each line is drawn between two nodes, representing two Internet Protocol addresses. The length of the lines is indicative of the delay between the nodes, and colours indicate the approximate geographic addresses of the addresses.

this responsibility rests upon Public Safety, the Canadian military only assumes the defence of their own networks, and relies upon internal security mechanisms of telecommunications companies and industry to ensure service to operations.

## Conclusion

After a century of defeats, both by the ruthless imperial powers of the 19th Century, and due to brutal internal revolutions, China does not hide its ambition to once again become the "Middle Kingdom" in the next century. Despite its claims of a "peaceful rise," there is plenty of bellicose rhetoric emanating from the official mouthpiece of the Chinese Communist Party (CCP), especially when it comes to territorial sovereignty, and this is exemplified by the ongoing dispute with the Japanese over the Senkaku/Diaoyu Islands. The consequences of being technologically inferior are still fresh in Chinese memory, and it is therefore not surprising that China has embarked upon an aggressive modernization campaign.

However, the successful adoption of information warfare as one of the means to achieve this aim is a remarkable way in which to conduct asymmetric warfare. Using low cost means, China may have successfully stolen billions worth of intellectual property and fuelled their national objectives, saving a crucial amount of time and money in research and development. The Chinese spatial program and the development of its aerospace industries are good examples of such rapid development, allowing the Chinese industry to undercut competition in world markets. In the meantime, China continues its effort on economic and political fronts by buying stakes in strategic sectors, and by pushing for decentralized control of the Internet.[63]

In modern militaries, which are dependent upon computer systems, it only makes sense for an adversary to target these systems. As long as the cost of conducting CNO remains lower than defence costs and has the ability to disrupt operations, attacks upon information systems are very plausible. Additionally, most of these systems are maintained by civilian industry, which may not consider operational security as their Number One priority. Attacking civilian critical infrastructure, which often supports military communications, may prove an effective power projection tactic against modernized democracies.

As Canada closes out its mission in Afghanistan after a decade of counter-insurgency operations, we may now encounter a completely new type of warfare. The CAF faces new budget restrictions, and large-scale new 'boots on the ground' military operations, while always possible, are perhaps somewhat unlikely in the immediate future. This slowdown may be the opportunity for the CAF to consider its role in cyber operations, which are often training-intensive, but are relatively low cost when compared to traditional deployments. It may also be valuable to estimate how an attack upon our networks, both unclassified and classified, would impact military operations. Within industry, exercises are conducted to simulate a major attack against power grids and to test the interrelationships between organizations.[64] Banks also have adopted their own exercises to continue services in case of a major cyber attack.[65] More than 20 nations *have integrated* or *are integrating* military units to conduct operations in cyberspace,[66] and as the leaks from the National Security Agency (NSA) are released, we can expect this number to grow rapidly. Could the CAF deploy troops should logistics systems be unavailable? Can we defend against a major cyber operation against our networks? Or even against Canada? Could the CAF be able to contribute to cyber offensive operations within a coalition? These are some of the questions that the CAF will now face.

CMJ

Shutterstock 120227461 by Stephen Finn

## NOTES

[1] John Markoff, "Vast Spy System Loots Computers in 103 Countries," *in The New York Times*, 29 March 2009, at http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=0.

[2] Ron Diebert and Rafal Rohozinski, "Part Two. *Tracking GhostNet: Investigating a Cyber Espionage Network* (Toronto: Information Warfare Monitor, 2009), pp. 43–44.

[3] Foreign Spies Stealing Us Economic Secrets In Cyberspace. (October 2011). *Office of the National Counter-intelligence Executive*, p. I, at <//www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.>.

[4] D. Charles, and P. Eckert, "China military hackers persist despite being outed by U.S.," Reuters, 6 November 2013, at http://www.reuters.com/article/2013/11/06/net-us-usa-china-hacking-idUSBRE9A51AN20131106.

[5] S. Hoe and D. Roebuck, *The Taking of Hong Kong Charles and Clara Elliot in China Waters* (Aberdeen, Hong Kong: Hong Kong University Press, 2009).

[6] J. Lovell, "Sweet-Talk and Sea-Slug," in *The Opium War* (London: Picador, 2012), pp. 114–115. (Original work published 2011).

[7] J.E. Bingham, *Narrative of the Expedition to China* (2nd edition). (London: H. Colburn, 1843), p. 217.

[8] J. Lovell, "Sweet-Talk and Sea-Slug," pp. 112-113.

[9] W.H. Hall and W.D. Bernard, *Narrative of the Voyages and Services of the Nemesis from 1840 to 1843* (2nd edition) (London: Henry Colburn, 1845).

[10] Sherard Osborn, "Past and Future British Relations with China," in *The Asiatic Journal and Monthly Register for British and Foreign India, China and Australasia*, 40, (n/d), p. 139.

[11] J. Lovell, "Qishan's Downfall," in *The Opium War*, pp. 85–86.

[12] J.C. Schencking, *The Rich Rewards and Rivalry of War, 1894–1904. Making Waves Politics, Propaganda, and the Emergence of the Imperial Japanese Navy, 1868–1922* (Stanford, CA: Stanford University Press, 2005), p. 78.

[13] S.M. Karmel, *The Goal: Overhauling China's Military Strategy. China and the People's Liberation Army: Great Power or Struggling Developing State?* (New York: St. Martin's Press, 2000), p. 26.

[14] Henry Kissinger, "Reagan and the Advent of Normalcy," in *On China* (New York: Penguin Press, 2011), p. 396.

15 D. Xiaoping, "Respect Knowledge, Respect Trained Personnel," in *People's Daily*, 24 May 1977, at http://english.peopledaily.com.cn/dengxp/vol2/text/b1110.html.

16 J.D. Spence, "Redefining Revolution," in *The Search for Modern China* (New York: Norton, 1990), p. 655.

17 C. Cox, N. Dicks, P. Goss, D. Bereuter, J.V. Hansen, J.M. Spratt Jr. *et al.*, "PRC Acquisition of U.S. Technology," in *U.S. National Security and Military/Commercial Concerns with the People's Republic of China* (Washington, DC: US Government, 1999), pp. 10–14.

18 S.M. Karmel, "The Goal…," p. 35.

19 T.M. Cheung, "The Structure of the Military Business Complex and its Key Corporation," in *China's Entrepreneurial Army* (Oxford, UK: Oxford University Press, 2001), p. 59.

20 "Huawei: The Long March of the Invisible Mr. Ren," in *The Economist*, 2 June 2011, at http://www.economist.com/node/18771640.

21 T.M. Cheung, "The Structure of the Military Business Complex…," p. 60.

22 Q. Liang and W. Xiangsui, *Unrestricted Warfare*, at http://www.cryptome.org/cuw.htm.

23 J. Mulvenon and R.H. Yang, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age* (Santa Monica, CA: RAND, 1999), pp. 175–185.

24 "Grasp New Features, Adopt New Concepts – Discussion of People's War under Conditions of Informationization," in *China National Defense News*, 15 October 2003.

25 Ke Chen, "Grasp New Features, Adopt New Concepts – Discussion of People's War Under Conditions of Informationization," in *Guofang Bao*, 2003.

26 Fu Minghe, "Information Operations and Innovative Concepts," in *Jiefangjun Bao* (2003).

27 M.A. Stokes, J. Lin, and L.R. Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," in *Project 2049 Institute*, 11 November 2011, at http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

28 *Ibid*, pp. 7-11.

29 "APT 1 – Exposing One of China's Cyber Espionage Units," in *Mandiant*, 19 February 2013, at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

30 Mark A. Stokes and L.C. Russell Hsiao, "Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests" in *Project 2049 Institut*e, 29 October 2012.

31 Bundesministerium des Innern, (2010). Spionage und sonstige nachrichtendienstliche Aktivitäten. *Verfassungsschutzbericht 2009* (Berlin: Bundesministerium des Innern, 2010), p. 341.

32 S. Doherty, J. Gegeny, B. Spassojevic and J Baltazar, "Hidden Lynx – Professional Hackers for Hire," in *Symantec*, 17 September 2013, p. 7, at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf.

33 C. Qingmei and X. Xuepeng, *Xinxi Anquan Jiaoxue Xitong Shixun Jiaocheng* (Beijing: China Machine Press, 2012).

34 S. Gorman, "Chinese Hackers Suspected In Long-Term Nortel Breach," in *Wall Street Journal*, 14 February 2012, at http://online.wsj.com/news/articles/SB10001424052970203363504577187502201577054.

35 J. Munson, "Canadian Energy Sector Rife with Chinese Cyberespionage: Reports," in *iPolitics*, 18 October 2012, at http://www.ipolitics.ca/2012/10/18/canadian-energy-sector-rife-with-chinese-cyberespionage-reports/.

36 N. Thornburgh, "Inside the Chinese Hack Attack," in TIME.com, 25 July 2005, at http://content.time.com/time/nation/article/0,8599,1098371,00.html.

37 "NetTraveler is Running! – Red Star APT Attacks Compromise High-Profile Victims," in *Securelist.com*, 4 June 2013, at http://www.securelist.com/en/blog/8105.

38 "APT 1 – Exposing One of China's Cyber Espionage Units," in *Mandiant*.

39 K. Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," in Wired.com, 10 January 2012, at http://www.wired.com/threatlevel/2010/01/operation-aurora/.

40 "The Elderwood Project," in *Symantec*, 6 September 2012, at http://www.symantec.com/connect/blogs/elderwood-project.

41 "Night Dragon," in *McAfee*, 10 February 2011, at http://www.mcafee.com/ca/about/night-dragon.aspx.

42 N. Villeneuve, J.T. Bennette, N. Moran, T. Haq, M. Scott and K. Geers, "Operation Ke3chang: Targeted Attacks Against Ministries of Foreign Affairs," in *FireEye*, 10 November 2013, at http://www.fireeye.com/resources/pdfs/fireeye-operation-ke3chang.pdf.

43 G. Weston, "Foreign Hackers Attack Canadian Government," in *CBCnews*, 16 February 2011, at http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618.

44 E. Chien and G. O'Gorman, "The Nitro Attacks – Stealing Secrets from the Chemical Industry," in *Symantec*, 1 September 2011, at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

45 S. Doherty, J. Gegeny, B. Spassojevic, and J. Baltazar, "Hidden Lynx – Professional Hackers for Hire," *Symantec*, September 17, 2013, at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf.

46 "Lab Global Research And Analysis Team (GReAT). The Icefog APT: A Tale of Cloak and Three Daggers," in *Kaspersky Lab*, at http://www.securelist.com/en/downloads/vlpdfs/icefog.pdf.

47 B. Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent," in *Krebs on Security*, 26 September 2012, at http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent./

48 S. DeWeese, B. Krekel, G. Bakos and C. Barnett, *Timeline of Significant Chinese Related Cyber Event 1999–Present. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: U.S. – China Economic and Security Review Commission, 2009), pp. 67-74.

49 "Pay raise of 50% for Chinese Soldiers," in *Asia News*, 24 March 2009, at < http://www.asianews.it/news-en/Pay-raise-of-50-for-Chinese-soldiers-14809.html>.

50 A. Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits," in *Forbes*, 23 March 2012, at http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

51 L. Bilge and T. Dumitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World," in *Carnegie Mellon—Electrical and Computer Engineering*, 16 October 2013, at http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf.

52 "Pay Rates," in Government of Canada, *National Defence* (n.d.), at < http://www.forces.gc.ca/en/caf-community-pay/pay-rates.page>.

53 K. Wilhoit, "The SCADA That Cried Wolf: Who Is Really Attacking Your ICS Devices Part 2," in *Trend Micro* (n.d.), pp. 16–17, at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-scada-that-didnt-cry-wolf.pdf.

54 Office of the U.S. Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: Department of Defense, 2013), pp. 36–37.

55 Office of the U.S. Secretary of Defense, *Annual Report to Congress on The Military Power of the People's Republic of China* (Washington, DC: Department of Defense, 2007), p.22.

56 "New Situation, New Challenges and New Missions," in *Ministry of National Defense*, 16 April 2013, at http://eng.mod.gov.cn/Database/WhitePapers/2013-04/16/content_4442752.htm.

57 "China scrambles jets in air zone to monitor US and Japanese planes," in *BBC News*, 29 November 2013, at http://www.bbc.co.uk/news/world-asia-25155605.

58 J.T. Quigley, "Diaoyu Island Assault: PLA-Designed Video Game Simulates Sino-Japanese Conflict," in *The Diplomat*, 2 July 2013, at http://thediplomat.com/china-power/diaoyu-island-assault-pla-designed-video-game-simulates-sino-japanese-conflict/.

59 J. Mulvenon, and R.H. Yang, pp. 184–185.

60 B. Moore, "Defense Resource Management Information System, Enabling the Transformation of Supporting Operations," in *IBM*, November 2012 , at < http://ibm.co/1ev5ko1>..

61 "Shamoon Virus Targets Energy Sector Infrastructure," in *BBC News*, 17 August 2012, at http://www.bbc.co.uk/news/technology-19293797.

62 J. Leyden, "South Korea Data-Wipe Malware Spread by Patching System," in *The Register*, 25 March 2013, at http://www.theregister.co.uk/2013/03/25/sk_data_wiping_malware_latest/.

63 J. Robertson, "U.S. vs. China, Russia in Battle for Control Over the Internet," in *Bloomberg.com*, 12 December 2012, at http://go.bloomberg.com/tech-blog/2012-12-12-u-s-vs-china-russia-in-battle-for-control-over-the-internet/.

64 M.L. Wald, "As Worries Over the Power Grid Rise, a Drill Will Simulate a Knockout Blow," in *The New York Times*, 16 July 2013, at < http://www.nytimes.com/2013/08/17/us/as-worries-over-the-power-grid-rise-a-drill-will-simulate-a-knockout-blow.html>.

65 H. Jones and S. Slater, "Cyber 'War Games' to Test London Banks: Response," in *The Globe and Mail*, 7 November 2013, at http://www.theglobeandmail.com/report-on-business/international-business/european-business/simulated-cyber-attack-to-test-london-banks-response/article15313266/.

66 Institute of Land Warfare, "Computer Network Operations: A Critical Element of Current and Future Military Operations in Combating the Asymmetrical Threat," Association of the United States Army, November 2012, at http://www.ausa.org/SiteCollectionDocuments/ILW%20Web-ExclusivePubs/Background%20Briefs/bb96.pdf