ANALYTIC OF CHINA CYBERATTACK

Robert Lai, CISSP-ISSAP, ISSEP, CAP, CEH, CSSLP[1]
and Syed (Shawon) Rahman, Ph.D.[2]

[1]School of Business & Technology, Capella University, Minneapolis, MN 55402, USA
rlai@capellauniversity.edu
[2]Assistant Professor, University of Hawaii-Hilo, Hilo, USA
and Adjunct Faculty, Capella University, Minneapolis, USA
SRahman@Hawaii.edu

ABSTRACT

China cyberattack has become aggressive, disruptive, stealthy, and sophisticated. Apparently, China's advantage is more on the cognitive domain than technical domain since information systems security is art and science—in some case, it is more art than science. Knowledge is the best weapon for cyber warfare since one of the Sun Tze's Art of War principles is "know your enemy". Therefore, an analytic of China cyberattack must scrutinize the national interest, goals and philosophies, culture, worldview, and behavioral phenomena of China.

KEYWORDS

China, Cyberattack, Cyberattack, Analytic, Strategic Advantage, Information Warfare

1. INTRODUCTION

China cyberattack is an emerging threat to the national security of the U.S. since the U.S. has no dominance in cyber domain, while China goes on the offensive in cyberspace. The air, land, sea, and space domains are all interdepended on cyber infrastructure in order to be effective. A full-spectrum cyber security strategy depends on an analytic of China cyberattack by examining its dynamic strategic advantage and critical competitive advantage. In the literature review and analysis section, the comprehensive view of China cyberattack covers: (a) cyber espionage by China; (b) cyberattack for political and military goals; (c) cyber assaults; (d) China as an emerging cyberpower; (e) challenges; (f) extreme information warfare; (g) asymmetric attack; (h) dynamic strategic advantage; (i) Sun Tzu's Art of War; (j) Mao's theory of strategy and tactics; (k) Go (Wei-Ch'i)—a Chinese strategic game; (l) Chinese martial arts—the Tao (way) of fighting; (m) abductive reasoning—smart thinking; (n) critical competitive advantages; and (o) soft power—knowledge. In addition, there is an overview of the cyberspace operations of the U.S. Finally, the recommendation is an analytical framework to include analysis patterns for the U.S. analysts, strategists, and decision makers to examine the circumstances of China cyberattack in the cognitive domain in order to come up with a deterrent strategy.

1.1. Background information

As early as 1993, two RAND researchers, John Arquilla and David Ronfeldt, published "Cyberwar is Coming!" in Comparative Strategy journal, and referred to the cyberwar in conducting, and preparing to conduct nonconventional military operations according to information-related principles [1]. The U.S. demonstrated cyber war capability in Operation Desert Storm that shocked the China's People Liberation Army (PLA), but the event inspired and

DOI : 10.5121/ijma.2012.4304

enlightened the PLA to take the lessons learned, and press forward on Revolution in Military Affairs (RMA)—a transformation from conventional warfare to unconventional warfare with information and communication technology (ICT) [2], [3]. According to the report “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation” prepared for the U.S.-China Economic and Security Review Commission, China’s increasing capabilities in cyber warfare have posed emergent threats to the national interest of the U.S. [4]. The Iraq Wars, Kosovo, and Afghanistan wars resulted in China realizing U.S. overwhelming information superiority in modern warfare with command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR). Nevertheless, C4ISR as net-centric has a dependence on space and cyberspace, which make the two domains the most vulnerable. In Sun Tzu’s Art of War, one of the principles is to strike where the enemy is most vulnerable. China understands this strategy profoundly, and develops capabilities in parallel to exploit these vulnerabilities. China has attained shashoujian (killer weapon) as a deterrent tool to against the United States, and the shashoujian will be very effective as a secret and disruptive weapon for asymmetric attack to the cyber infrastructure of the U.S. China’s shashoujian means more than “assassin’s mace” that it is a vital concept on combining Western technology with Eastern wisdom into an array of secret weapons and military doctrines [5]. China is taking the stance that the best defense is offense, where its space and cyberspace program (elements of shashoujian) are focused on offensive strategies. Besides anti-satellite (ASAT) missile, PLA has also developed a unique carrier-killing missile with multiple payloads called the Dong Feng 21D to intimidate the U.S. Navy in the event of potential conflict over Taiwan or North Korea [6]. There have been many incidents of hacking by Chinese to the U.S. defense and civilian government networks, but China denies the allegation since cyber attribution—positive identification of the agent/actor responsible for the attack—is still a challenge [7]. However, Kevin Coleman, a Senior Fellow at the Technolytics Institute, said that China has the intent and technological capabilities necessary to carry out a cyberattack anywhere in the world at any time [8]. The critical infrastructure of the U.S. that include financial network, communication, internet, Supervisory Control and Data Acquisition System (SCADA) controlled water and power grids, and defense network are all vulnerable to cyberattack. China Cyber Warfare has both strategic and competitive advantages.

2. LITERATURE REVIEW AND ANALYSIS

2.1. China cyberattack

2.1.1. Cyber espionage by China

It is easy to conduct espionage on cyberspace by nation-states or state-sponsors since adversaries can take advantage of vulnerabilities to steal trade secret, intellectual property, financial data, personal identifiable information, and classified data from corporations, institutions, defense contractors, or the government. Cyber espionage is part of cyberattack since its intent is to exfiltrate information from target for latter attack. The Technolytics Institute has estimated that Department of Defense (DoD) has lost over 20-27 terabytes of data in 2007 [9]. Adversaries will use stolen military and industry secrets to aid their future cyberattack. China is the most active nation-state on cyber espionage activities with a “grain of sands” approach—steals as much data as possible, and infers valuable information from the stolen data [10]. Most experts believe that China is responsible for the ten worst computer hacking events: (1) Titan Rain; (2) State Department’s East Asia Bureau; (3) Offices of Rep. Frank Wolf; (4) Commerce Department; (5) Naval War College; (6) Commerce Secretary Carlos Gutierrez and the 2003 blackout; (7) McCain and Obama presidential campaigns; (8) Office of Sen. Bill Nelson; (9) Ghostnet; and (10) Lockheed Martin’s F-35 program [11]. Cyber espionage is a threat that gives adversaries the asymmetric advantages on gaining critical technology, trade secret, intellectual property, financial data, personal identifiable information (PII), and classified data from corporations, institutions, defense contractors, or the government so that they can level the playing field.

In 2011, a sophisticated hack on U.S. Chamber of Commerce system went undetected for over six months with evident linked to China [12]. The hackers hijacked some known Chamber employees' Yahoo and Hotmail addresses, and sent phishing emails to all Chamber staffs with malicious links to steal their credentials (e.g., login name, password), and install malware on their computer systems [13]. This type of social engineering technique is spear phishing that exploits the cognitive biases of uninformed users. The attack applied an advanced persistent threat (APT) technique to implant a Trojan with command and control capability to pinpoint the targets—key Asia-policy staffs of the U.S. Chamber of Commerce. The breach was gigantic since the hackers had unrestricted access to three million members of the U.S. Chamber of Commerce, which is the America's top business-lobbying group [14].

Bloomberg reported that China-based hackers did another aggressive attack on iBahn—a major internet service provider (ISP) that offers internet broadband service to guests of Marriott hotel, and other hotel chains [15]. Over 760 entities (e.g., companies, research universities, ISPs) are members of the iBahn's network. Travelers use iBahn service for internet service, and access their office's internal networks while traveling. The network's breach at this level offers hackers the easy man-in-the-middle attack, and by-pass most security controls (e.g., encryption, multiple factor authentication). In a written statement, iBahn has denied any network's breach at all, but anonymous sources confirmed that the attack originated in China [16]. Without any doubt, the characteristics of attack have matched closely to the style of Chinese hackers, which are aggressive, holistic, stealthy, and sophisticated.

Cyber espionage activities by Chinese hackers are on the rise, and it is widespread to all American business, industry, and government sectors. Attack on supply-chain is not a task that non-nation-state hackers can easily achieve since it requires huge resources and technical skills. There are proofs that Chinese hackers have targeted the supply-chain. In 2008, the Federal Bureau of Investigation (FBI) conducted Operation Cisco Raider to uncover 3,500 counterfeit Cisco network devices valued at $3.5 million from China [17]. These fake network devices (e.g., router, switch) were purchased by DoD, federal government agencies, defense contractors, universities, and financial institutions, which could make them vulnerable to cyberattack since it would be very difficult to detect malware in the firmware. Technolytics has suggested that cyber espionage is a $1.5 trillion problem, and there is no easy countermeasure solution [9]. The grand scale of cyber espionage activities by China is far-reaching: data breach can include mass quantity of personal/customer data, financial data, and trade secrets on compromised systems.

2.1.2. Cyberattack for political and military goals

"The Chinese are the first to use cyber-attacks for political and military goals", says James Mulvenon, an expert on China's military and director of the Center for Intelligence and Research in Washington [18]. After the Google China Hack, Google's Corporate Development and Chief Legal Officer, Drummond wrote, "we have discovered that the accounts of dozens of U.S.-, China- and Europe-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. These accounts have not been accessed through any security breach at Google, but most likely via phishing scams or malware placed on the users' computers." Dr. Toshi Yoshihara, a Research Fellow and resident expert on security issues in the Asia-Pacific region at the Institute for Foreign Policy Analysis, has pointed out that China has demonstrated an intense fascination with information warfare (IW) in his monograph "Chinese Information Warfare: A Phantom Menace or Emerging Threat" [19].

2.1.3. Cyber assaults

In November 2006, Chinese hackers prompted Navy college site closure [20]. The Chinese hackers have increased their interest in getting information on military network infrastructure. In addition, the Defense Information Systems Agency's Non-classified Internet Protocol Router Network (NIPRNET) is a prime target for many hackers to exploit. The PLA understands that the attacks on NIPRNET might effectively affect the military's logistics system [21]. Data mining might even infer classified information from data on unclassified network. The office of Department of Defense (DoD) Secretary, Robert Gates, was hacked by PLA in 2007, and the unclassified network was forced to shut down for a week long [22].

2.1.4. Hidden dragon—invisible capabilities

China cyber capabilities are far-reaching and complex. For example, GhostNet penetrated over 1,000 compromised computers in 103 countries, and targeted a network of high-value targets (e.g., diplomatic, political, economic, and military) [23]. GhostNet is a robust and sophisticated network that the investigation team has located including a covert design with advanced botnet capabilities (e.g., delivery mechanisms, data retrieval and control system, and capable of taking full control of affected systems) [24]. Even one year after the discovery of this botnet, researchers have identified unknown branch of GhostNet that primarily targets India using cloud-based social networking services (e.g. Twitter, Facebook, and Google) to perform command and control (C2) [25]. Compared to the first cyber weapon—logic bomb—by CIA 30 years ago that damaged a Soviet computer-controlled pipeline system, GhostNet is an advance cyber weapon that can cause more harm according to the cyber weapon definition on the Cyber Commander's Handbook by Technolytics [9], [26]. Moreover, China is very adaptive to stay on top of cyber weapons evolution with rapid advancement in a new kind of malicious code—known as advanced persistent threats (APTs). Operation Shady RAT (RAT stands for remote access tool) has been undetected for over five years until recently, and it was effective to hit 72 organizations and 14 countries with focus on government agencies and defense contractors [27]. The Operation Shady RAT uses a basic spear-phishing attack—fake email to steal credential—to use encrypted HTML comments in Web pages for a command channel to the infected machine that can evade detection. The breath-taking aspect of this operation is the grand scale, which McAfee's researchers have access to petabytes of stolen data on gaining access to one specific command and control server used by the intruders [27]. This operation must require a huge number of people to run the operation. Who else besides China has the resources to do it? The answer seems to be too obvious.

2.1.5. China as an emerging cyberpower

Kuebl [28] defines cyberpower as "the ability to use cyberspace to create advantage and influence events in all the operational environments and across the instruments of power." The U.S. has mighty power to dominate land, sea, air, and space domain. Cyberspace is not a domain that the U.S. has dominance. Does U.S. have the cyberpower like seapower, airpower, and spacepower? U.S. does not have cyberpower like other domains yet. It seems to be an arms race for the front-runners, China and Russia, to complete with the U.S. in the 21st century. In a network centric (net-centric) warfare, the integration of land, sea, air, and space domains with the cyber domain is critical to command and control. The U.S. military needs freedom of movement in each domain, but the cyber domain is the most important core component of the Global Information Grid (GIG). Both China and Russia have gained ground on cyberspace with both cyberattack and cyber intelligence capabilities. China is working on a trusted infrastructure with a secure operating system with its own derivative trusted platform module (TPM)—trusted cryptography module (TCM) to enforce the chain of trust, which will deny the attack by other countries [29] [30]. China has extensive experience in packet inspection and capture at its edge routers to the Internet since the beginning of its connection to external networks. The Estonian and Georgian cyber war experiences have demonstrated that Russia has a team of sophisticated hackers to conduct effective cyber operations against Estonia and Georgia. In the conflict with Estonia, attackers focused the attack on strategic targets with a mass cyber assault using botnet that traced back to IP addresses from 178 countries; in the conflict with Georgia, civilian of Russia attacked Georgian strategic targets with hacking tools and information by hacktivists in an innovative way [31]. Moreover, both China and Russia have the language advantage over the U.S. since there are few U.S. cyber security professional can speak and read either Chinese or Russian. Under the political, informational, military, and economic (PIME) model, China is an emerging cyberpower that has a higher PIME's overall rating [28].

In the situation report of "The Day After…in Cyberspace" exercise held at the National Defense University on June 3, 1995, Molander [32] and his research team predicate that China can leads economic growth in Asia, expand military power in the region, and advance in offensive and defensive cyber capabilities in the early 21st century. China indeed has not disappointed Molander on achieving the top contender in cyber warfare, and has even become a game-changer. In addition, China is the first cyberpower with a preemptive strategy [33].

2.1.6. Challenges

Cyber Warfare is a reality not fiction. Both the Estonia and Georgia conflicts are recent examples of cyber warfare. There are many stakeholders with individual interest on cyberspace for their own economy, safety, and political objectives. The U.S. national interest is for its own long-term economy, safety, and political objectives. The movie War Games has a famous tagline: "the only winning move is not to play", but it is not really an option since the U.S. is a digital nation that is cyber dependent [34]. Cold War's strategy and tactic are no way to be effective in cyber warfare since Cold War has few predictable threats and actors (i.e., nation-state) while cyber warfare has many unpredictable threats and actors (i.e., nation-state, non-state). Unlike Cold War, Cyber War is dynamic and multifaceted. China advance in cyber warfare is problematic to the national security and national interest of the U.S.

Being reactive, the full spectrum cyber security approach is hard to counter the asymmetric attack by the master—China. The *Yin-Yang* concept is a good representation of China's cyberattack that is both heuristic and systematic. It might worthwhile to ponder the strategy, tactical, operational, and patterns of China Cyber Warfare using an analytic framework to predict China's next move in order to deny, degrade, detect, and counter cyberattack by China effectively.

2.1.7. Extreme information warfare

Effectiveness of information warfare used in the Gulf War has enlightened PLA to engage in information warfare development two decades ago. In 1996, Wei Jincheng, a military strategist wrote to use the Internet as a platform to engage in warfare without stepping out of the door in the Liberation Army newspaper [35]. "Thanks to modern technology, such as the development of information carriers and the Internet, many can now take part in fighting without even having to step out of the door," noted Wei Jincheng, a military strategist, in the Liberation Army Daily newspaper in 1996. Wei's idea on information warfare (IW) received the buy-in from PLA Major General Wang Pufeng—the founder of Chinese IW. According to Yoshihara [19], China takes full attention on each major aspect of IW (i.e., PSYOPS, denial, and deception), and modernize its cyber force with advanced cyber weaponry in order to assure victory in a cyber conflict. Dr. Yoshihara has agreed that China has incorporated IW as an integral part of RMA (personal communication). According to the paper, "China Debates the Future Security Environment" [36], China's RMA scenarios against an opponent (e.g., U.S., Russia, and Japan) will:

- Close an information gap
- Network all forces
- Attack the enemy C3I to paralyze its operations
- Pre-empt enemy attacks
- Use directed energy weapons
- Use computer viruses
- Use submarine-launched munitions
- Use antisatellite weapons
- Use forces to prevent a logistics buildup
- Use special operations raids

Chinese military strategists have laid out a concept of operations (ConOps) to integrate information technology and IW stratagems to its defense, but Western analysts and policy decision makers have not played close attention to the intent of PLA's RMA. Based on China's RMA scenarios, China has chosen to take offensive role on IW.

China's approach on IW is extreme since it is comprehensive to target all five fighting domains (i.e., land, sea, air, space, and cyberspace). It is goal-oriented to build up capabilities in each domain with innovative and disruptive solutions. China takes bold move like GhostNet and Google China Hack, which surprises many Western analysts. For example, GPS jammer is low cost, but it is disruptive enough to put its adversary at disadvantage state.

2.1.8. Asymmetric attack

Dr. Lai and Dr. Yoshihara have both agreed with the author that the Chinese martial arts are analogous to asymmetric attack. Unlike boxing a sport with formal rules, Chinese martial arts is a full contact combat technique with unrestricted rule. A Chinese martial artist with knowledge of acupuncture points can bring an opponent to his knees with a minimum of movement [37]. It is the same analogy on exploitation of vulnerabilities in an information system.

Asymmetric warfare strategies and capabilities are the core elements in PLA's RMA for improving its war-fighting abilities and national security. Therefore, cyber warfare capabilities with asymmetric advantage will receive the most resources (e.g., budget, labor). The conflict of the Taiwan Strait is the best example of asymmetric warfare with cyber operations to deter or delay U.S. involvement.

The use of a low-tech method or device to attack the high-tech system is a Mao's notion of "using the inferior to overcome the superior" [38]. Even Sun Tzu's notion of winning a battle without fighting through superior opponent is an asymmetric warfare [19].

2.1.9. Dynamic strategic advantage

Chinese strategic culture has a collection of theories, doctrines and methodologies as strategic advantage. The collection has Chinese characteristics that include: (a) Sun Tzu's Art of War; (b) Mao's theory of strategy and tactics; (c) Go—a game of encirclement and capture; (d) fighting concept of Chinese martial arts—the Tao of fighting; and (e) abductive reasoning—smart thinking.

2.1.9.1. Sun Tzu's Art of War

Sun Tzu's Art of War provides a body of knowledge on strategic and tactical planning that is suitable for conventional and un-conventional warfare. Consisting of 13 chapters, the Art of War covers many factors that decide victory or defeat according to: (a) political climax; (b) weather;

(c) battlefield's terrain; (d) logistic; (e) intelligence; (f) war stratagems; (g) deception; (h) quality of warfighters; and (i) people's support [39]. One of the key principles is to strike where the enemy is most vulnerable, which is very effective on cyberspace. The Art of War gives China the qualitative edge on strategic and tactical planning.

2.1.9.2 Mao's theory of strategy and tactics

Mao Zedong's people's war is famous in guerrilla warfare on attack that is both holistic and agile. People-centric is a focal point of Mao's theory of strategy and tactics to mobilize the mass to defeat a superior enemy [40]. The China Cyber Warfare has reflected the characteristics of Mao's theory of strategy and tactics, that the cyber commanders must: (a) select and advance to the spot where the resistance is the weakest; (b) avoid or bypass a strong defense and to assault a weak spot; (c) make a detour in order to attack the rear or flank of the enemy's position; (d) confuse the enemy by attacking at one point to divert his attention while actually advancing on another; and (e) knew how to spy on their enemies and the activities of their clandestine operation [41].

2.1.9.3. Go (Wei-Ch'i)—a Chinese strategic game

Go is a strategic skill game on a 19x19-grip board to train analytic skill, which requires analytical thinking to contemplate means to end using nested loop evaluation. Hathaway [42], says "the best of Wei-Ch'i masters play multiple strategies on multiple boards—all at the same." Military strategy planners (masters of Go) can plan simultaneous attack like multi-threading on a supercomputer. The handicapping system of Go permits a weaker player to play with a strong player as a way to practice asymmetric attack. The philosophies of *Yin-Yang* and Daoism are in perfect harmony with Sun Tzu's dialectic views on the way of war and diplomacy—applied on Go—like water that: (a) it has no constant shape; (b) it is fluid; (c) it is dynamic; and (d) it is capable to penetrate and attack the hard and strong [43]. The strategy framework of China's PLA is rather complex like multiple strategies for multiple Go's boards all at once.

2.1.9.4. Chinese martial arts—the Tao (way) of fighting

The fighting concept of Chinese martial arts involves a strategy that aligns with the *Yin-Yang* principle, but it is also very adaptive to the challenger. The best Chinese martial artists can visualize their plan of actions regularly against imaginative opponents before a real combat [44]. Situation awareness and swift decision might be the factors to win or lose. Martial arts train the minds and bodies of practitioners to cultivate concentration, patience, persistent, focus, and agility [45]. The martial arts' qualities are the characteristics of Chinese warfighters including the cyber warriors.

2.1.9.5. Abductive reasoning—smart thinking

Most people reason with either inductive or deductive logic, but Chinese reason like abductive logic. Ross [46] summarizes abductive logic:

- D is a collection of data (facts, observations, givens)
- H explains D (would, if true, explain D)
- No other hypothesis can explain D as well as H does
- Therefore, H is probably true

Abductive reasoning is a good tool to formulate strategy since it allows assumption to be proved in the future, and it is a challenge to the deductivism. China's IW stratagems made the correct assumption about cyber war twenty years ago.

2.1.10. Critical competitive advantages

Resources and capabilities are major elements to establish competitive advantage. China has gained many competitive advantages. It is impossible to list of them all in this report since it is hard to verify and validate the emerging resources and capabilities. This report only includes some samples of China's competitive advantages that are critical to support its strategy.

Anti-satellite (ASAT) weapon: the successful ASAT missile test event on January 17, 2007, showed that China has already mastered the capability in counter-space by using ballistic missiles to shoot down spy satellites in low earth orbit [47]. China's ASAT test has just aligned with its strategy to decapitate, paralyze, disintegrate, and blind the adversary [48]. This ASAT test demonstrated the vulnerability of US satellites in low earth-orbit (LEO) medium earth-orbit (MEO) as force enhancement for: (a) intelligence, surveillance, and reconnaissance (ISR); (b) integrated tactical warning and attack assessment; (c) command, control, and communications (C3); (d) position, velocity, time, and navigation (i.e., global position system (GPS)); (e) GPS navigation for smart bombs and troops; and (f) environmental monitoring [49]. From China's perspective, the ASAT test is a military hedge to the U.S. space dominance, and it is a strong signal on active defense [50].

Breakthrough in Cryptanalysis—the Message Digest 5 (MD5) and Secure Hashing Algorithm Version 1 (SHA1) for digital signature are both broken. Commonly, data integrity relies on a secure hash function like MD5 or SHA1. The hash is similar to fingerprint that should be unique since the message digest algorithms are one-way computation on the data and it is hard to produce the same hash after a change in the data [51]. According to Rivest [52], "the MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA." As per Eastlake and Jones [53], "the SHA-1 is based on principles similar to those used by Professor Ronald L. Rivest of MIT when designing the MD4 message digest algorithm [MD4] and is modeled after that algorithm." Prof. Wang Xiaoyun at Shandong University led a research team to break MD5 by collision attack, and did the same for SHA1 afterward [54].

In 2010, China's Tianhe-1A supercomputer was the most powerful computer in the world with 2.57 petaflops performance [55]. High performance computer (HPC) could provide capabilities in design, development, manufacturing, performance, and testing of weapons and weapons platforms [56]. HPC in the realm of national security could make great progress in:

- Nuclear, chemical, and biological weapons
- Tactical aircraft (e.g., unmanned aerial vehicle (UAV))
- Cruise and ballistic missiles
- Submarines
- Anti-submarine warfare
- Command, control, and communications
- Information warfare
- Cryptography

Internet censorship with Chinese characteristics—most analysts only focus on freedom of speech, but they ignore that China's censorship capability offer them an asymmetric advantage. China has begun censorship activities even since Chinese start using Internet. From capturing every packet to inspecting the content, and applying rules to blockage, China has gained much practical experience from censorship activities. China's Internet infrastructure has a complete, multi-layer, multi-channel, and distributed content monitor system built-in to perform deep packet inspection, which can be a defense as well [57]. According to Wu [57], Internet censorship by the Chinese regime features the following four Chinese characteristics:

- The combination of universal filtering and manual spot-check.
- Blurring the rules and launching underground manipulation among departments. The criterion for "harmful information," "sensitive information" and "subversion behavior" is not defined within the 50 plus law-cases.
- Inefficient administration and discouraged legal system causes difficulty in seeking litigation when the authorities illegally run down or delete information from the websites in China. It is difficult to search for definitive terms such as who executes the punishment. What is the law entry that is violated? By which law is the principal punishment being executed? These problems are distinctively manifested in those websites of academy, law and rights safeguarding.
- Scouting and banning protest activities and the political movements supported by oversea forces. For the sake of "its own security," authorities do not consider influences acting upon the international society.

A report by the OpenNet Initiative in 2009 has stated that China's Internet filtering system is the most complex, advanced, and pervasive in the entire world [58]. It is not an easy task to monitor Internet’s traffic on over 500 million Internet users (a.k.a. netizens) in China without a sophisticated filtering system.

Mao’s doctrine on people’s war works well for the Chinese hackers. Are they organized? No, they are ad-hoc, but patriotism can mobilize them to strike the common adversary for free. The pool of hacking talents is proportion to the China’s Internet user’s base. The numbers of freelance, patriotic, and professional hackers in China must be huge. Based on the sophistication of Titan Rain, GhostNet and Operation Aurora attacks, Chinese hackers have expertise in custom malware coding [59].

2.1.10.1. Soft power—knowledge

Knowledge is power, and China is making rapid progress in systems engineering, and information and communication technology. In net-centric warfare (NCW), C4ISR is the force multiplier for joint warfighting to support net-centric operations—see first, understand first, and act first [60]. Platforms of five military operational domains (i.e., land, sea, air, space, and cyber) depend on the C4ISR capabilities to interoperate effectively and efficiently. Integration of C4ISR—system of systems—depends on a state-of-the-art systems engineering. To successfully delivery a capability or solution, solid systems engineering and project management are both critical.

In the 1970s, Dr. H. S. Tsien—a major innovator behind the missile and space programs of both the United States and China—established scientific framework for Systems Engineering (SE): (a) the concept and methods of "systematology" as basic studies of systems science; and (b) the field of "systematics" as the link between systems science and scientific philosophy [61]. Dr. Tsien’s idea on systems engineering is far-reaching to apply the SE concept on space program, military science and technology, human factors, social development, economy, complex systems (i.e., system of systems), information science, system management, operation research, system control, communication technology, and automation science [62]. In addition, Chinese systems engineers have achieved major systems development and integration for space and advance weapon systems using the oriental Wu-li Shi-li Ren-li (WSR) system methodology proposed by Dr. Tsien around 1990s [63]. The Chinese SE is a combination of both synthetic and analytic. Dr. Tsien’s questioned the methodology on how to solve open complex giant system problems that should be human-centric by utilizing the oriental humanity in relationship with social-cultural setting. In the Encyclopedia of Life Support Systems, Zhu [64] says, “sustainable development decisions are seen by the Oriental WSR approach as participation processes conditioned and shaped by a dynamic web of wuli (relation with the world), shili (relation with the mind) and renli (relation with others)......the Oriental WSR with its unique cultural imprints will enrich and improve humankind's ability towards integrated decisions and policies.” Ren means people in Chinese language that is the corner stone of Confucianism. Appling ancient wisdom, oriental culture, and abductive reasoning with contemporary systems methodology is the Chinese approach on complex systems development process.

2.2. Cyberspace operations of the U.S.

Cyberspace is a new fighting domain and virtual battlefield, which can harm the critical infrastructures of the U.S. since they are all networked to the cyberspace and vulnerable to cyberattack. According to the Homeland Security Presidential Directive 7 (HSPD 7), there are 18 sectors in the critical infrastructures of the U.S. (Table 1. Critical Infrastructure Sectors) that are targets of cyberattack [65]. Most people are not aware of the emerging cyber-physical systems (CPS)—integrations of computation with physical processes—in our daily life. It is possible to have physical consequences and casualties without kinetics attack following a cyberattack like the Stuxnet as a cyber-weapon to sabotage the Iranian nuclear facility in Natanz [66]. The physical infrastructure (e.g., government facilities, railroad, pipelines, and ports), critical infrastructure/key resources (CIKR) (e.g., energy, information technology, banking and finance) and cyber infrastructure (e.g., software, hardware, internet, information service, and control systems) are interdependent. Cyber Operations are complex and dynamic for defense and offense. In this chapter, the focus is information-centric on the perspectives of the U.S. military and national policy. Cyber Operations include information operations (IO), computer network operation (CNO), computer network defense (CND), computer network attack (CNA), and computer network exploitation (CNE).

Agriculture and Food	**Banking and Finance**	**Chemical**
Commercial Facilities	Communications	Critical Manufacturing
Dams	Defense Industrial Base	Emergency Services
Energy	Government Facilities	Healthcare and Public Health
Information Technology	National Monuments and Icons	Nuclear Reactors, Materials and Waste
Postal and Shipping	Transportation Systems	Water

Table 2. Critical Infrastructure Sectors

2.2.1. Information operations and cyberspace operations

The latest version of Joint Publication 3-13—a joint doctrine—defines information as a strategic resource, vital to national security, and military operations depend on information and information systems for many simultaneous and integrated activities [67]. IO utilizes an array of capabilities like electronic warfare (EW), CNO, psychological operations (PSYOP), and military deception (MILDEC), to affect the adversary’s information environment while protecting one’s own information environment in addition with information assurance (IA) and CND [68]. However, the U.S. Government Accountability Office (GAO) has a new set of key definitions (Table 3. DoD Cyberspace-Related Terms and Definitions) in the GAO-11-421 and GAO-11-695R reports of Defense Cyber Efforts. Consequently, the Cyberspace Operation is a replacement of IO for the rest of this paper to avoid confusion.

Term	Definition
Cyberspace	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
Cyberspace Operations	The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.
Computer Network Attack (CNA)	Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
Computer Network Defense (CND)	Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.
Computer Network Exploitation (CNE)	Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
Computer Network Operations (CNO)	Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.
Full-Spectrum Cyberspace Operations	The employment of the full range of cyberspace operations to support combatant command operational requirements and the defense of DOD information networks. This includes efforts such as computer network defense, computer network attack, and computer network exploitation.
Global Information Grid (GIG)	The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems.
Information Assurance	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.

Table 3. DoD Cyberspace-Related Terms and Definitions

2.2.2. Cyberspace environment

The environment for cyberspace operation—cyberspace environment—has still captured the three dimensions of information environment: physical, informational, and cognitive [67]. However, the U.S. Army offers a newer model of cyberspace environment with three layers (i.e., physical, logical, and social) made up of five components (i.e., geographic, physical network, logical network, cyber persona, and persona), which is a structural representation of cyberspace [69]. The three layers of cyberspace can map to the three aspects of information systems security: people, operations, and technology. Technology aspect contains both physical network component (e.g., hardware) and logical network component (e.g., software). Operations aspect (e.g., process, policy, standard) matches with logical network components. People aspect ties closely with the social layer's persona and cyber persona components. People, operations, and technology aspects interweave the three layers of cyberspace.

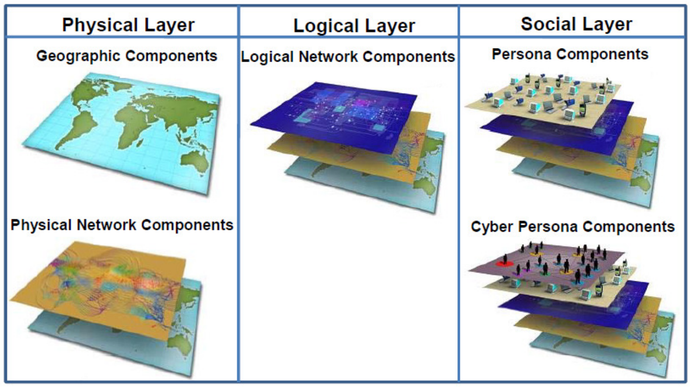

Figure 1. The three layers of cyberspace, Adapted from *Cyberspace Operations Concept Capability Plan 2016-2028* (No. TRADOC Pamphlet 525-7-8). (2010)

Physical layer. The physical layer consists of two components: geographic and physical network. Geographic component provides geographical information of the network elements . The physical network component encompasses all hardware and infrastructure of information and communication technology.

Logical layer. The logical layer comprises the logical network component, which contains the logical (i.e., technical) configuration information among network elements, applications, and infrastructure. The logical network component provides the link between physical layer and social layer. Security control (e.g., access control list) is also a kind of logical network component. In fact, all technical entities are logical.

Social layer. The social layer includes the cyber persona component and the persona component with consideration of cognitive perspectives (e.g., value, thinking). Persona component consists of real person with positive identity; cyber persona component represents a logical identity (e.g., email address, phone number) of a person.

2.2.3. Global Information Grid (GIG)

The objective of GIG is to allow global "information sharing" capability of command, control, computer, communication, intelligence, surveillance and reconnaissance (C4ISR) among all DOD Components and mission partners in a network-centric environment [70]. This is a change from "need to know" to "need to share"—a paradigm shift. On the other hand, the DOD expects GIG that can enhance interoperability among DOD's many information systems and weapon systems for business and warfighting. GIG has six operational capability areas (OCAs): (1) Assured Information Sharing (AIS); (2) Assured Mission Management (AMM); (3) Confidentiality (CON); (4) Highly Available Environment (HAE); (5) Defend the GIG (DTG); and (6) Integrity and Non-Repudiation (INR). The GIG is a critical asset to the U.S. cyber domain.

2.2.4. Computer Network Operation (CNO)

CND comprises of IA, CND, CNA, and CNE. IA and CND are defense functions of CNO; CNA and CNE are offense functions of CNO. There are little public information about the details of CNA and CNE since they are rather sensitive.

Information Assurance (IA). The strategy of IA is defense-in-depth on three aspects: people, technology and operations. The IA posture is "people executing operations supported by technology" universally for any organization [71]. Overlapping approaches and layers of protection with the principle aspects of IA (Table 4. Principal Aspects of IA) will assure availability, integrity, authentication, confidentiality, and nonrepudiation to the information and information systems [71]. IA also depends on supporting infrastructures like key management infrastructure (KMI)/public key infrastructure (PKI), and detect and respond to meet the security objectives. IA is an essential protect and defend component of CND. Yet, defense-in-depth is not perfect since it introduces layered vulnerabilities. For example, sandbox security has stack-overflow vulnerability and inherent software flaws [72].

People	Technology	Operations
Policies and Procedures	IA Architecture framework areas	Security Policy
Training and Awareness	IA criteria (security, interoperability, and PKI)	Certification and accreditation
Physical security	Acquisition integration of evaluated products	Readiness assessments
Personnel security	System risk assessments	Security management
System security administration		Key management
Facilities Countermeasures		Attack sensing and warning response
		Recovery and reconstitution

Table 4. Principal Aspects of IA

2.2.5. **Computer Network Defense (CND)**

CND have the tasks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. The protection activity of CND utilizes the IA principles and approaches. The Framework of CND Services describes the actions to prevent or minimize computer network attacks that would disrupt, deny, degrade, destroy, exploit, and access the information systems or networks (

Table 5. Framework of CND Services). However, CND is rather ineffective since it relies on known vulnerabilities and virus signatures primary. Intrusion detection system (IDS) alerts, firewall and network traffic logs, and host system logs all depend on analysis by human, but there is no guarantee on unpublished signatures.

Computer Network Defense Services			
Protect	**Monitor, Analyze, and Detect**	**Respond**	**Capability Sustainment**
Vulnerability Analysis and Assessment (VAA) Support	Network Security Monitoring/Intrusion Detection	Incident Reporting	MOUs and Contracts
CND Red Teaming	Attack Sensing and Warning (AS&W)	Incident Response	CND Policies/Procedures
Malware Protection Support	Indications and Warning (I&W)/Situational Awareness	Incident Analysis	CND Technology Development, Evaluation and Implementation
Subscriber Protection Support and Training			Personnel Levels and Training/Certification

Computer Network Defense Services			
Information Operations Condition (INFOCON) Implementation			Security Administration
Information Assurance Vulnerability management (IAVM)			CNDSP Information Systems

Table 5. Framework of CND Services

2.2.6. **Computer Network Attack (CNA)**

The Deceive, Deny, Disrupt, Degrade, Destroy (D5) effects are the objectives of a CNA. CNA uses the same methodology for hacking:

- Reconnaissance
    - Active/Passive
- Scanning/Fingerprinting
    - IP Address, Ports, Services
- Penetration
    - Network Level, Operating System Level, Application Level
- Attack
    - Upload files, Alter data, Download files/data
- Own the system
    - Covering Tracks, Clean up log file

When the target is an infrastructure like SCADA, a coordinated physical attack is a viable alternative to digital attack. Electromagnetic pulse (EMP) weapon can severely damage advanced telecommunications, energy supply systems, information and computer networks, and transportation systems from a distance of several miles [9]. CNA targets are both physical and informational domain.

2.2.7. Computer Network Exploitation (CNE)

The primary target of CNE is informational domain. The objective is to collect intelligence by using information systems and computer networks to gather data from target or adversary information systems or networks [67]. Even the action of CNE is very similar to certain aspects of CNA, it is because only certain organizations are permitted to conduct CNA legally [68]. Interestingly, CNE has no such restriction.

2.3. Analytical framework

Cyber warfare is a complex and dynamic subject with increasing variables and changing landscape. There is sufficient of objective evident to prove that China Cyber Warfare is a threat to the U.S. Is it really a Black Swan event for China's rise in cyberspace? No, China's rise in cyberspace is inevitability a perfect storm instead. Then, how should the U.S. cope with the perfect cyber storm? The U.S. analysts, strategists, and decision makers need a methodology on how to examine the circumstances of China Cyber Warfare in the cognitive domain, and get situation awareness on the threat in order to come up with a deterrent strategy. The purposed methodology is an analytical framework to include analysis patterns to support analytic abductively.

Cyberspace is a construct by human. Human perception is the dynamic of cyber warfare. Apparently, China's warfare advantage is more on the cognitive domain than technical domain since information systems security is art and science—in some case, it is more art than science. Knowledge is the best weapon to cyber warfare since one of the Sun Tze's Art of War principles is "know your enemy". The analysis-synthesis should focus on soft information related to their cognitive domain:

- National interest
- Goals and philosophies
- Culture
- Worldview
- Behavioral phenomena
- Analytical techniques
- Utilization of current and potential capacities

2.3.1. Concepts and Techniques

2.3.1.1. Sensitivity analysis

Analysis patterns are more qualitative than quantitative. The expected results depend on China's intention (i.e., likely to do) and capability (i.e., capable to do). In fact, there are uncertainty to China's intention and capability. Sensitivity analysis—what-if analysis—is a technique to support decision making under uncertainty by varying the change in input. In this case, the sensitivity analysis can model the likelihood of cyberattack—threat, and economic and social impact of attack for analytical result on the uncertainty—next cyberattack by China.

Often, sensitivity analysis is not suitable to qualitative analysis, but there is a workaround to any variable or factor that is descriptive. According to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30: Risk Management Guide for Information Technology Systems , risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization [73]. The threat likelihood has Low, Medium, and High level. The threat likelihood level can be interpreted in terms of probability with 0.1 for Low, 0.5 for Medium, and 1.0 for High [73]. In risk analysis, it is purposely not to set the threat likelihood to have zero value since it means no such probability. Likewise, the value of threat impact can be assigned to 10 for low, 50 for medium, and 100 for high [73]. Together, threat likelihood and threat impact form a 3X3 risk-level matrix for low risk at 1-10, medium risk at 10-50, and high risk at 50-100. For a High threat likelihood (1.0) and High threat impact (100), the risk level is 1.0 x 100 = 100 = High risk. The numerical rating of risk-level matrix helps in explaining the degree of risk and its criticality. The threat likelihood and threat impact are scenario for what-if analysis to model the risk factor of each asset. The analysis can provide the basis on safeguard justification, risk mitigation decisions, and resource prioritization according to the risk factor.

For analytic purpose, the sensitive analysis can take into consideration of other properties or factors like demographic, cyber offensive capabilities, cyber defensive capabilities, and cyberattack vectors. The unpredictable will become more predictable by using the right data, and applying the correct analysis.

2.3.1.2. Avoiding surprise

The fact is clear that China is on the rise with increasing confidence, while the prospect of U.S. is declining [74]. U.S. as the sole superpower is unsustainable forever. In an essay in a special edition of Harvard Magazine, Taiwan's President Ma Ying-jeou [75] predicted that China would lead Asia to be the center of the global economy, and become a power in the region in the early 21st century. Multipolar world order is the new order. National interest of the U.S. has to make adjustment, while China is aggressively challenging the unipolar world order of the U.S.

2.3.1.3. Disruptive technology

According to the Avoiding Technology Surprise for Tomorrow's Surprise for Tomorrow's Warfighter [76], three sources can cause technology surprise: (a) product and process technology breakthroughs; (b) new uses of existing technology; and (c) unexpectedly rapid progression to the operation use of the technology. Analytical thinking about the three sources will bring a new understanding about China's advantage for offensive cyberattack. Wolf [77], says "technological change can undermine companies and industries with little warning. The challenge, of course, is anticipating, detecting, and addressing disruptive change before the impact undermines the business, costing money and jobs." Being anticipatory is the right way to project disruptive change.

2.3.1.4. Intelligence diversity

Chinese language is high context, while English is low context. English speakers tend to expect explicit in communication, but Chinese speakers understand the implicit meaning between words. Language is a barrier for the U.S. to obtain good intelligence form China. In addition, culture bias is a problem to prevent understanding the goals and philosophies of China. For example, Admiral James R. Hogg has considered that Asians only use inductive approach, but Chinese also use abductive thinking process beside inductive [76]. Without the language and culture skill, analysts cannot produce the correct analyses by word pattern analysis. Word pattern analysis is a way to do statistical analysis on keyword from Chinese open source (e.g., technical publication, newspaper, website) to obtain cyber intelligence. Good analytic on China Cyber Warfare requires good source of cyber intelligence.

2.3.1.5. Cultural and political context

There are more Chinese students studying the English and American culture than American students are studying Chinese and Chinese culture. This is an asymmetric disadvantage to the U.S. with fewer intelligent analysts that can articulate the context of Chinese language and culture [76]. It is a bias to use the concept of American-centric to analyze Chinese culture and value since Chinese perspective is different from the Western perspective. Asians look for the relationship of the entities (nonlinear) in the question; Westerners look for similarity of the entities (linear) in the question.

The Hainan Incident—a U.S. Navy EP-3 surveillance plane and a People's Liberation Army Navy (PLAN) F-8 jet collided over the South China Sea on April 1st, 2001—has demonstrated a tension between China and U.S. [78]. After the near-fatal collision, the U.S. aircraft with 24 military service men and women made an emergency landing at Lingshui military airfield on Hainan Island. The PLAN pilot, Lt. Cmdr. Wang Wei, lost in the South China Sea, and Chinese President Jiang Zemin conferred upon Wang a special honor title "Guardian of the Seawaters and Airspace" [79]. In this face-off,. China detained the 24 crewmembers, and demanded U.S. to apologize for the incident [80]. The U.S. asked China to return the crewmembers, and not to tamper with the EP-3. Secretary Powell made it clear that U.S. would have nothing to apologize, and only expressed regret over the missing PLAN pilot [80]. China insisted the right to inspect the EP-3. In Beijing on April 11, the U.S. Ambassador Prueher sent a letter of regret—the "Letter of Two Very Sorries"—expressed a "very sorry" for the loss of the pilot, Wang Wei, and another "very sorry" for the EP-3's unauthorized emergency landing on Haina [81]. China accepted the letter, and agreed to release the crews out of humanitarian considerations. In English, "very sorry" is not an apology, but China considers that "very sorry" is an acknowledgement of a serious misbehave. China did not allow the EP-3—an $80 million aircraft—to fly out of China even the Pentagon insisted the EP-3 was "definitely repairable to be flown" [80]. Finally, the U.S. Embassy in Beijing agreed to disassemble the EP-3, and transport the pieces back to the U.S. on a Russian charter cargo plane. Lockheed Martin got the contract to perform the work for over $5.8 million to reassemble and repair the plane [80]. Without an apology, China made it costly for the U.S. to recover the EP-3. Which country won in this incident? The U.S. considered that the resolution was a win, but China had access to the EP-3 with advance surveillance systems for eleven days. Due to the death of Wang Wei, China's hackers lashed out with web defacements and distributed denial-of-service (DDoS) attack against the U.S. federal government and defense web sites as retaliation [82].

3. CONCLUSION

The author of Nation-state Cyber Strategies: Examples from China and Russia, Timothy Thomas [33], said, "Chinese cyber capabilities have become more visible and troubling. China has launched an unknown number of cyber reconnaissance and offensive events with unknown intent against a variety of countries." "Unknown" is the keyword in his message. So, it is the unknown "unknown" that bothers most people about China Cyber Warfare. In fact, there are patterns of China cyber operations to trace, and the patterns should represent some meanings. China has always denied any cyberattack with the involvement of the government or military since there is still the challenge to attribution. China has the attacker advantage on asymmetric warfare. Demographics, modern technology, systems engineering, and Eastern wisdom (e.g., stratagem, philosophies) are force multiplier to China's superiority on cyberspace.

In this paper, the analyses supported that China has dynamic strategic advantage and critical competitive advantages on Cyber Warfare. The U.S. needs a comprehensive and innovative strategy on China Cyber Warfare by taking an analytical approach to counter or deter China from future cyberattack. Lacking in cyber intelligence about China is a shortcoming of the U.S. cyberspace strategic planning. Cyberspace is an emerging phenomenon by human, therefore human/cognitive perception should be the focus of a cyber-strategy.

REFERENCES

[1]. J. Arquilla and D. Ronfeldt, "Cyberwar is Coming!," 1993. [Online]. Available: http://www.rand.org/pubs/reprints/RP223/. [Accessed: 28-Apr-2012].

[2]. T. Galdi, "CRS 95-1170F: Revolution in Military Affairs?," 11-Dec-1995. [Online]. Available: http://www.fas.org/man/crs/95-1170.htm. [Accessed: April 11, 2012].

[3]. L. Kamienski, "The RMA and War Powers," Strategic Insights, vol. 2, no. 9, 2003.

[4]. B. Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," DTIC Document, 2009.

[5]. J. E. Bruzdzinski, "Demystifying Shashoujian: China's 'Assassin's Mace' Concept," Sep-2004. [Online]. Available: http://www.mitre.org/work/best_papers/04/bruzdzinski_demystify/bruzdzinski_demystify.pdf.

[6]. E. Talmadge, "Chinese Missile Could Shift Pacific Power Balance," 06-Aug-2010. [Online]. Available: http://www.csmonitor.com/From-the-news-wires/2010/0806/Chinese-Missile-could-shift-Pacific-power-balance. [Accessed: May 11, 2012].

[7]. D. D. Clark and S. Landau, "Untangling Attribution," 2010. [Online]. Available: http://www.nap.edu/openbook.php?record_id=12997&page=25. [Accessed: 11-Dec-2011].

[8]. K. Coleman, "Defense Tech: China's Cyber Forces," 08-May-2008. [Online]. Available: http://defensetech.org/2008/05/08/chinas-cyber-forces/. [Accessed: May 20, 2012].

[9]. B. Engelmann and P. Cordaro, Eds., Cyber Commander's Handbook. 2010.

[10]. D. Sevastopulo, "Hackers breach White House system," Financial Times, United Kingdom, London (UK), p. 6, 2008.

[11]. J. Rogin, "The Top 10 Chinese Cyber Attacks (that we know of)," 22-Jan-2010. [Online]. Available: http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of.

[12]. T. Greene, "Chinese Hack on U.S. Chamber of Commerce Went Undetected for 6 Months," 21-Dec-2011. [Online]. Available: http://podcasts.infoworld.com/d/security/chinese-hack-us-chamber-commerce-went-undetected-6-months-182435?_kip_ipx=816219059-1326849376&source=rss_security. [Accessed: 18-Jan-2012].

[13]. G. Smith, "Chinese Hackers Used 'Spear Phishing' To Attack U.S. Chamber Of Commerce," 21-Dec-2011. [Online]. Available: http://www.huffingtonpost.com/2011/12/21/chinese-hackers_n_1163524.html.

[14]. "US Chamber of Commerce Hit by Chinese Hackers," 21-Dec-2011. [Online]. Available: http://thehackernews.com/2011/12/us-chamber-of-commerce-hit-by-chinese.html. [Accessed: 1/18/2012].

[15]. M. Riley and J. Walcott, "China-Based Hacking of 760 Companies Shows Cyber Cold War," 14-Dec-2011. [Online]. Available: http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html. [Accessed: 24-Jan-2012].

[16]. J. Kirk, "iBahn, Supplier of Hotel Internet Services, Denies Breach," 15-Dec-2011. [Online]. Available: http://www.networkworld.com/news/2011/121511-ibahn-supplier-of-hotel-internet-254110.html.

[17].J. H. Follett, “Cisco Channel At Center of FBI Raid On Counterfeit Gear,” 12-May-2008. [Online]. Available: http://www.crn.com/news/networking/207602683/cisco-channel-at-center-of-fbi-raid-on-counterfeit-gear.htm;jsessionid=48luh8qHEoP9Xfs8H0xvEg**.ecappj01. [Accessed: 25-Jan-2012].

[18].R. Marquand and B. Arnoldy, “China Emerges as Leader in Cyberwarfare,” 14-Sep-2007. [Online]. Available: http://www.csmonitor.com/2007/0914/p01s01-woap.html. [Accessed: 11-Dec-2011].

[19].T. Yoshihara, Chinese Information Warfare a Phantom Menace or Emerging Threat? Carlisle, PA :: Strategic Studies Institute, U.S. Army War College,, 2001.

[20].John Tkacik, Jr., “Trojan Dragon: China’s Cyber Threat,” 08-Feb-2008. [Online]. Available: http://www.heritage.org/research/reports/2008/02/trojan-dragon-chinas-cyber-threat. [Accessed: 11-Dec-2011].

[21].China’s Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities. Washington, DC: , 2008.

[22].Deutsche Presse-Agentur, “China’s Army Hacked Pentagon Network,” 05-Sep-2007. [Online]. Available: http://www.military.com/NewsContent/0,13319,148037,00.html. [Accessed: 11-Dec-2011].

[23].K. Geers, Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, 2011.

[24].R. Rohozinski and R. Deibert, “Tracking GhostNet: Investigating a Cyber Espionage Network.” Information Warfare Monitor, 29-Mar-2009.

[25].T. Friedman, “Chinese Based Botnet Discovered, Larger Than Previously Thought,” 07-Apr-2010. [Online]. Available: http://www.neowin.net/news/chinese-based-botnet-discovered-larger-than-previously-thought. [Accessed: 11-Dec-2011].

[26].“Cyberwar: War in the Fifth Domain,” 01-Jul-2010. [Online]. Available: http://www.economist.com/node/16478792. [Accessed: 11-Dec-2011].

[27].D. Alperovitch, Revealed: operation shady RAT. McAfee, 2011.

[28].D. Kuebl, “Chapter 2: From Cyberspace to Cyberpower: Defining the Problem,” in Cyberpower and national security, 1st ed., Washington D.C.: National Defense University Press ; Potomac Books, 2009.

[29].B. Gertz, “Washington Times: China Blocks U.S. from Cyber Warfare,” 12-May-2009. [Online]. Available: http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/. [Accessed: 13-Jun-2010].

[30].H. Li, H. Hu, and X.-F. Chen, “Research on Compliant Testing Method of Trusted Cryptography Module,” Chinese Journal of Computers (计算机学报), vol. 2009, Apr. 2009.

[31].R. Heickerö, “Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations,” FOI, Swedish Defence Research Agency, User Report, Mar. 2010.

[32].R. Molander, Strategic Information Warfare : A New Face of War. Santa Monica CA: RAND, 1996.

[33]. L. Thomas, “Chapter 20: Nation-state Cyber Strategies: Examples from China and Russia,” in Cyberpower and national security, 1st ed., Washington D.C.: National Defense University Press ; Potomac Books, 2009.

[34].J. Badham, War Games. MGM, 1983.

[35].M. Moore, “China Sees Electronic Spying as Area Where It can Defeat America,” 29-Mar-2009. [Online]. Available: http://www.telegraph.co.uk/news/worldnews/asia/china/5071300/China-sees-electronic-spying-as-area-where-it-can-defeat-America.html. [Accessed: 11-Dec-2011].

[36]. “China Debates the Future Security Environment.” [Online]. Available: http://www.globalsecurity.org/military/library/report/2000/part09.htm. [Accessed: 12-Dec-2011].

[37].E. Ahrari, “China’s Preoccupation with Asymmetric War | Small Wars Journal,” Mar-2007. [Online]. Available: http://smallwarsjournal.com/jrnl/art/chinas-preoccupation-with-asymmetric-war. [Accessed: 12-Dec-2011].

[38].G.-W. Jinn, “China’S Development Of Asymmetric Warfare And The Security Of Taiwan,Repubulic Of China,” Naval Postgraduate School, Monterey, Ca, 2004.

[39].H. Jianying, “The Art of War by Sun Zi: A Book for All Times,” Jun-2002. [Online]. Available: http://www.chinatoday.com.cn/English/e20026/sunzi1.htm. [Accessed: 13-Dec-2011].

[40].Z. Mao, The Art of War, Special ed. El Paso, Tx: El Paso Norte Press, 2005.

[41].Samuel B. Griffith, Sun Tsu: The Art of War. Oxford ;;London ;;New York: Oxford university press, 1971.

[42].M. E. Hathaway, “Strategic Advantage: Why America Should Care About Cybersecurity,” Oct-2009. [Online]. Available: http://belfercenter.ksg.harvard.edu/publication/19640/strategic_advantage.html.

[43].D. Lai, “Learning from the Stones: A Go Approach to Mastering China’s Strategic Concept, Shi,” 01-May-2004. [Online]. Available: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=378.

[44].W. Lo, “Lama Martial Arts,” unpublished.

[45].M. Lee, Black Belt Negotiating : Become a Master Negotiator Using Powerful Lessons from the Martial Arts. New York: American Management Association, 2007.

[46].J. M. Ross, “Informatics Creativity: A Role for Abductive Reasoning?,” Communications of the ACM, vol. 53, no. 2, pp. 144–148, Feb. 2010.

[47].[47] C. Covault, “Chinese Test Anti-Satellite Weapon,” 17-Jan-2007. [Online]. Available: http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/CHI01177.xml.

[48].J. E. Bruzdzinski, “Hearing on: Military Modernization and the Cross-Strait Balance Remarks as Presented before the U.S.-China Commission,” 05-Sep-2008. [Online]. Available: http://www.uscc.gov/hearings/2004hearings/written_testimonies/04_02_06wrts/bruzdzinski.htm.

[49].“Center for Space Studies - Military Force Enhancement,” 13-Nov-2006. [Online]. Available: http://space.au.af.mil/enhance.htm. [Accessed: 18-Dec-2011].

[50]. E. D. Hagt, New Frontier in Sino-U.S. Relations: Challenges in Space. 2007.

[51]. H. Tipton and Krause, Micki, Eds., Information Security Management Handbook. [Boca Raton, FL.] :: Auerbach,, 2007.

[52]. R. Rivest, “The MD5 message-digest algorithm,” 1992.

[53]. D. Eastlake and P. E. Jones, “US secure hash algorithm 1 (SHA1),” 2001.

[54]. “Breakthrough in Cryptanalysis,” 2007. [Online]. Available: http://www.nsfc.gov.cn/Portal0/InfoModule_480/24255.htm. [Accessed: 18-Dec-2011].

[55]. “BBC News - China’s Tianhe-1A crowned supercomputer king,” 16-Nov-2010. [Online]. Available: http://www.bbc.co.uk/news/technology-11766840. [Accessed: March 18, 2012].

[56]. “Washingtonpost.com: The Cox Report,” 25-May-1999. [Online]. Available: http://www.washingtonpost.com/wp-srv/politics/daily/may99/coxreport/chapter3.htm. [Access:4/18/2012].

[57]. Y. Wu, “The Epoch Times | Internet Censorship in China,” Sep-2006. [Online]. Available: http://www.theepochtimes.com/news/6-11-10/47995.html. [Accessed: 19-Dec-2011].

[58]. “OpenNet Initiative: Internet Filtering in China,” 2009. [Online]. Available: http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf. [Accessed: April 20, 2012].

[59]. J. Stewart, “Operation Aurora: Clues in the Code | Dell SecureWorks,” 19-Jan-2010. [Online]. Available: http://www.secureworks.com/research/blog/research/20913/. [Accessed: May 20, 2012].

[60]. National Research Council (U.S.), Army Science and Technology for Homeland Security. Washington, D.C. :: National Academies Press,, 2004.

[61]. “Omega Alpha Association: Honorary Members.” [Online]. Available: http://www.omegalpha.org/honorary-members.html. [Accessed: May 20, 2012].

[62]. H. S. Tsien, 论系统工程/《系统科学与系统工程》丛书—Systems Engineering. 湖南科学技术出版社, 1988.

[63]. J. Gu and X. Tang, “Wu-Li Shi-Li Ren-Li System Approach to a Major Project on the Research Of Meta-Synthesis System Approach,” International Journal of Knowledge and Systems Sciences, vol. 1, no. 1, pp. 70–77, 2004.

[64]. Z. Zhu, “WSR Decisions for a Sustainable Future.” [Online]. Available: http://www.eolss.net/Sample-Chapters/C02/E6-46-02-11.pdf. [Accessed: May 20, 2012].

[65]. “DHS | Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection,” 2008. [Online]. Available: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

[66]. R. M. Schneiderman, “New Computer Malware May Presage Another Cyberattack, Potentially on Iran - The Daily Beast,” 16-Nov-2011. [Online]. Available: http://www.thedailybeast.com/articles/2011/11/16/new-computer-worm-may-presage-another-cyber-attack-potentially-on-iran.html. [Accessed: May 25, 2012].

[67]. Joint Publication 3-13: Information Operations. 2006.

[68]. E. Armistead, Information Operations: The Hard Reality of Soft Power. Dulles Va. ;Poole: Brassey’s ;;Chris Lloyd, 2003.

[69]. “Cyberspace Operations Concept Capability Plan 2016-2028,” Ft. Monroe, VA, TRADOC Pamphlet 525-7-8, Feb. 2010.

[70]. Joint Vision 2020. Washington DC: Government Printing Office, 2001.

[71]. “Information Assurance Technical Framework 3.1,” Sep-2002. [Online]. Available: http://www.iacf.gov/iacf/documents/framework_3-1/index.cfm. [Accessed: 20-Jun-2009].

[72]. A. Podhradsky and C. Casey, “Security Sandbox Program: Defense-in-depth or Layered Vulnerabilities?,” Mar-2011. [Online]. Available: http://searchsecurity.techtarget.com/tip/Security-sandbox-program-Defense-in-depth-or-layered-vulnerabilities. [Accessed: 26-Jan-2012].

[73]. G. Stoneburner, A. Goguen, and A. Feringa, “NIST SP 800-30: Risk Management Guide for Information Technology Systems,” Jul-2002. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. [Accessed: May 25, 2012].

[74]. R. Handler, “Will the 21st century belong to China? Let the debates begin - World - CBC News,” 21-Jun-2011. [Online]. Available: http://www.cbc.ca/news/world/story/2011/06/21/f-vp-handler.html. [Accessed: May 25, 2012].

[75]. Y.-J. Ma, “Harvard in a Multipolar World | Harvard Magazine Sep-Oct 2011,” Sep-2011. [Online]. Available: http://harvardmagazine.com/2011/09/harvard-in-a-multipolar-world. [Accessed: May 25, 2012].

[76]. National Research Council (U.S.), Avoiding Technology Surprise for Tomorrow’s Surprise for Tomorrow’s Warfighter. Washington, D.C. :: National Academies Press,, 2010.

[77]. David Wolf, “Avoiding Technology Surprise for Tomorrow’s Warfighter « The Peking Review,” 01-Nov-2011. [Online]. Available: http://pekingreview.com/2011/01/01/avoiding-technology-surprise-for-tomorrows-warfighter/. [Accessed: May 25, 2012].

[78]. M. K. Lewis, “Analysis of State Responsibility for the Chinese-American Airplane Collision Incident, An,” NYUL Rev., vol. 77, p. 1404, 2002.

[79]. B. Gertz, “The Last Flight of Wang Wei,” Jul-2001. [Online]. Available: http://www.afa.org/_private/Magazine/July2001/0701china.asp. [Accessed: 27-Jan-2012].

[80]. S. A. Kan, R. Best, C. Bolkcom, R. Chapman, R. Cronin, K. Dumbaugh, S. Goldman, M. Manyin, W. Morrison, R. O’Rourke, and others, “China-US Aircraft Collision Incident of April 2001: Assessments and Policy Implications,” in CRS Report for Congress, 2001, p. 15.

[81]. J. Keefe, “A Tale of ‘Two Very Sorries’ Redux,” Far Eastern Economic Review, 21-Mar-2002.

[82]. M. Hvistendahl, “Hackers: the China Syndrome | Popular Science,” 23-Apr-2009. [Online]. Available: http://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome. [Accessed: 27-Jan-2012].

[83]. Halton, Michael and Rahman, Syed (Shawon); "The Top 10 Best Cloud-Security Practices in Next-Generation Networking"; International Journal of Communication Networks and Distributed Systems (IJCNDS); Vol. 8, Nos. ½, 2012, Pages:70-84, ISSN: 1754-3916

[84]. Mohr, Stephen and Rahman, Syed (Shawon);“IT Security Issues within the Video Game Industry”; International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 5, Oct 2011

[85]. Dees, Kyle and Rahman, Syed (Shawon);“Enhancing Infrastructure Security in Real Estate”; International Journal of Computer Networks & Communications (IJCNC), ISSN : 0974 – 9322

[86]. Hood, David and Rahman, Syed (Shawon);“IT Security Plan for Flight Simulation Program”; International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.1, No.5, Oct 2011

[87]. Schuett, Maria and Rahman, Syed (Shawon); “Information Security Synthesis in Online Universities”; International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011

[88]. Jungck, Kathleen and Rahman, Syed (Shawon); " Cloud Computing Avoids Downfall of Application Service Providers";International Journal of Information Technology Convergence and services (IJITCS), Vol.1, No.3, June 2011

[89]. Slaughter, Jason and Rahman, Syed (Shawon); " Information Security Plan for Flight Simulator Applications"; International Journal of Computer Science & Information Technology (IJCSIT), Vol. 3, No 3, June 2011

[90]. Rahman, Syed (Shawon) and Donahue, Shannon; "Converging Physical and Information Security Risk Management", Executive Action Series, The Conference Board, Inc. 845 Third Avenue, New York, New York 10022-6679

[91]. Jungck, Kathleen and Rahman, Syed (Shawon); " Information Security Policy Concerns as Case Law Shifts toward Balance between Employer Security and Employee Privacy"; The 2011 International Conference on Security and Management (SAM 2011), Las Vegas, Nevada, USA July 18-21, 2011

[92]. Benson, Karen and Rahman, Syed (Shawon); "Security Risks in Mechanical Engineering Industries", International Journal of Computer Science and Engineering Survey (IJCSES), ISSN: 0976-2760

[93]. Bisong, Anthony and Rahman, Syed (Shawon); "An Overview of the Security Concerns in Enterprise Cloud Computing "; International journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011

[94]. Mullikin, Arwen and Rahman, Syed (Shawon); "The Ethical Dilemma of the USA Government Wiretapping"; International Journal of Managing Information Technology (IJMIT); Vol.2, No.4, November 2010, ISSN : 0975-5586

[95]. Rahman, Syed (Shawon) and Donahue, Shannon; “Convergence of Corporate and Information Security”; International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010; ISSN 1947-5500

ACKNOWLEDGEMENTS

We would like to thank Dr. Toshi Yoshihara, John A. van Beuren Chair of Asia-Pacific Studies Strategy and Policy, and professor at the U.S. Naval War College, for his invaluable inputs to this paper.

We would like to thank Dr. David Lai, a research professor of Asian Security Studies at the Strategic Studies Institute of the U.S. Army War College, to share his viewpoints with us on U.S.-China security policy. We would like to thank Jeff Deifik, CISSP, Sr. Software Engineer, for his comments on this paper.

Authors’ Bio:

Robert Lai is a Sr. Cyber Security Engineer at an information technology company. He currently holds CISSP-ISSAP, ISSEP, CAP, CEH, and CSSLP certifications. He was one of the contributors who were instrumental in developing the Certified Secure Software Lifecycle Professional (CSSLP) certification. He is a member of the (ISC)2 Application Security Advisory Board and a founding member of EC-Council’s Scheme Committee. He received a master’s degree in Information Assurance and Security from Capella University.

Dr. Syed (Shawon) M. Rahman is an assistant professor in the Department of Computer Science and Engineering at the University of Hawaii-Hilo and an adjunct faculty of School of Business and Information Technology (SoBT) at the Capella University. Dr. Rahman’s research interests include software engineering education, data visualization, information assurance and security, web accessibility, and software testing and quality assurance. He has published more than 75 peer-reviewed papers. He is a member of many professional organizations including ACM, ASEE, ASQ, IEEE, and UPE.