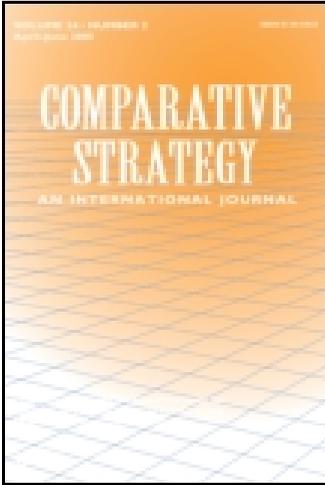


This article was downloaded by: [US Army War College]

On: 01 October 2014, At: 07:09

Publisher: Routledge

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Comparative Strategy

Publication details, including instructions for authors and subscription information:

<http://www.tandfonline.com/loi/ucst20>

Cyberwar: The United States and China Prepare For the Next Generation of Conflict

George Patterson Manson III ^a

^a Public and International Affairs Department George Mason University Fairfax , Virginia, USA

Published online: 09 May 2011.

To cite this article: George Patterson Manson III (2011) Cyberwar: The United States and China Prepare For the Next Generation of Conflict, *Comparative Strategy*, 30:2, 121-133, DOI: [10.1080/01495933.2011.561730](https://doi.org/10.1080/01495933.2011.561730)

To link to this article: <http://dx.doi.org/10.1080/01495933.2011.561730>

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at <http://www.tandfonline.com/page/terms-and-conditions>

Cyberwar: The United States and China Prepare For the Next Generation of Conflict

GEORGE PATTERSON MANSON, III
Public and International Affairs Department
George Mason University
Fairfax, Virginia, USA

In recent years the People's Republic of China has garnered international attention for its aggressive and often sophisticated employment of cyber capabilities against domestic and international targets alike. With increasing frequency, the targets of Chinese cyber operations are American companies or government networks. If the United States and China find themselves in conflict in the coming decades, this newest arena of operations, cyberwarfare, will play a decisive role in determining the outcome. This article examines the relative cyber strengths and weaknesses each country commands today, and offers policy recommendations for the improvement of the United States' own cyberwar capabilities.

Introduction

In June 1999, following the accidental bombing of the Chinese Embassy in Belgrade by U.S. warplanes during the NATO air campaign in the Balkans, Chinese nationalists took to the Internet, targeting U.S. and allied Web sites with denial-of-service (DOS) attacks, bringing down some Web sites and defacing others in protest for the bombing. Two years later, in April 2001, following the collision of a U.S. reconnaissance aircraft and a PLAAF coastal defense fighter over the sea south of Hainan Island, these Chinese “hacktivists” struck again, defacing numerous U.S. government Web sites and even briefly disrupting service to the webpage of the White House.¹ While these two cyber incidents did not do any serious damage to American Internet infrastructure or disrupt any critical functions, they were the first overt cyber attacks upon the United States by citizens of the People's Republic of China (PRC).

Analysts now appreciate that the military and civilian leadership of the PRC have been engaged in a concerted effort to build Chinese cyberwarfare capabilities for nearly two decades. The wake-up call for Chinese leaders came in the early 1990s, when military planners in Beijing watched the U.S.-led coalition dismantle Saddam Hussein's army with relative ease, seizing control of the battlefield with superior information systems and “smart” strike capabilities made possible by the integration of computer network technology and military hardware, enabling complex logistical and combat operations and providing coalition forces with unmatched near real-time intelligence. The war demonstrated to Chinese leaders just how far behind the state-of-the-art their own conventional capabilities had become, and Chinese strategists were soon referring to Operation Desert Storm by the name *zhongda bianq* (重大变革), the “great transformation.”²

The Chinese People's Liberation Army (PLA) has been engaged in a wide-ranging modernization process since the early 1990s, and the military has enjoyed a steadily increasing annual budget in recent years, growing from approximately \$45 billion in 1996 to over \$150 billion in 2010, a more than three-fold growth in the last decade and a half.³ This modernization effort, which reflects the PLA leadership's desire to develop a more

professional and capable military in keeping with the realities of the twenty-first-century battlefield, has resulted in a significant downsizing of the total force, improved training for all service branches, acquisition of foreign military technology systems and platforms, and extensive investment in Chinese domestic military-production capabilities. The push for modernization has also included the development of an advanced cyberwarfare capability. The Pentagon's annual assessment of Chinese military strength determined in 2009 that the PLA has established "information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks." Chinese Computer Network Operation (CNO) capabilities have evolved to include strong network attack, exploitation, and defense means.⁴

The United States, once the unchallenged master of what the Pentagon calls "net-centric" warfare, has not moved quickly to meet this Chinese challenge. Richard Clarke, formerly President George W. Bush's cyber "czar," and the author of a recently published book on cybersecurity, laments that successive administrations, despite being provided with ample evidence of American vulnerability to cyber attack, have not made cyberwar a strategic priority.⁵ Although in May 2010 President Obama authorized the creation of U.S. Cyber Command, a sub-unified command within the Department of Defense tasked with centralizing the military's cyber operations, little progress has been made in securing the United States' extensive network-integrated critical infrastructure, the vast majority of which is owned and operated by unprotected private-sector entities. President Obama's own cyber czar, Howard Schmidt, who assumed his position a year after Obama came to office, remains a little-known figure with no budgetary authority.⁶ Washington's slow progress in addressing the growing cybersecurity challenge over the last decade has occurred during a period in which Beijing has been aggressively building its own cyberwarfare capabilities. The People's Republic, some experts have asserted, will spend more money developing Internet technologies than will the United States by the year 2017.⁷ Many analysts now believe that the PLA has already acquired, through its development of strong cyberwarfare capabilities, the means to asymmetrically challenge the United States in the event of a kinetic conflict between the two states.

This article examines the emerging threat that Chinese cyberwarfare capabilities pose to the United States' national security. The first section will explore the relative offensive and defensive cyberwarfare strengths that the PRC and the United States wield today, and the degree of cyber dependence under which each nation operates. The second section evaluates the PRC's intent in developing such capabilities, and the third examines the recent history of cyber attacks perpetrated by the PRC's cybersecurity forces. The fourth section explores the difficulty of cyber attack attribution, which makes cyberwarfare such a uniquely dangerous tool of coercion, and the final section offers some policy recommendations to address this emerging threat.

Cyberwarfare Capabilities of Beijing and Washington Compared

Offensive Capabilities

The ruling Communist Party of China has developed its nation's cyber-offense capabilities through a number of pursuits, including the recruitment of citizen hacker groups, the creation and training of cyberwar military units, the distribution to the world market of compromised network hardware, and the placement of logic bombs and exploitation points throughout foreign networks.

The U.S.-China Economic and Security Review Commission estimates that China operates up to 250 groups of patriotic hackers who perform at the party's behest a wide

range of cyberwar functions, from harassment and monitoring of internal dissent, to the defacement of targeted foreign sites, to the execution of more complex cyber espionage and denial-of-service attacks. These Chinese hackers are not overtly linked to the government, yet, as Larry Wortzel of the Review Commission reflects, the hackers' "... persistent, systematic and sophisticated attacks, some of which have taken place in the United States, in China, in Germany, and in the United Kingdom, most likely are state-directed ... it is the organs of control and repression in China who most profit from such penetrations."⁸ It is these state-directed groups that were responsible for the attacks on U.S. sites in the wake of the 1999 embassy bombing and the 2001 EP-3 spy-plane incident.

The PLA has also created a number of uniformed cyberwarfare units, including the Technology Reconnaissance Department (3rd Department) and the Electronic Countermeasures and Radar Department (4th Department). These military units are augmented by personnel from the Ministry of State Security, the PRC's premier foreign and domestic intelligence organization, and cyber experts drawn from throughout the PRC's extensive network of state-owned enterprises.⁹ These cyber units are engaged on a daily basis in the development and deployment of a range of offensive cyber and information weapons, including "... planting information mines, conducting information reconnaissance, changing network data, releasing information bombs, dumping information garbage, disseminating propaganda, applying information deception, releasing clone information ... and establishing network spy stations."¹⁰ As the Pentagon's analysts state in their 2010 evaluation of China's military capabilities, numerous computer systems around the globe, including U.S. government systems, have been the target of Chinese offensive cyber operations, the principal focus of which, to date, has been the exfiltration of massive amounts of data of strategic or military utility.¹¹

The Chinese government has also sought to exploit its role as a major source of manufactured IT hardware to distribute compromised routers and servers abroad. In one known instance, Chinese companies sold reverse-engineered Cisco servers, either under the Cisco brand or relabeled as goods produced by China's own Hauwei company, to a number of western clients. Some of the compromised routers were ultimately sold to the U.S. Marine Corps, Air Force, and numerous defense contractors. A 2007 FBI report asserts that the compromised hardware could be used by foreign intelligence operatives to bring down networks or seriously weaken cryptographic systems.¹² It is likely that the Chinese government has sought in other as-yet undiscovered or undisclosed instances to leverage its role as a major player in the global IT supply chain to propagate similarly compromised hardware and software abroad.¹³

Finally, China's cyber operatives are engaged in lacing the United States' network-dependant infrastructure, including the power grid, water and sewage utilities, the financial system, and air traffic control systems, among others, with malicious code known as "logic bombs," which could be activated in a time of conflict to wreak widespread and indiscriminate havoc on the U.S. homeland.¹⁴ As Deputy Undersecretary of Defense Robert Lawless admitted, the Chinese have developed a "... very sophisticated capability to attack and degrade our computer systems ... to shut down our critical systems."¹⁵

Despite this rapid improvement in PRC offensive cyber capability, Clarke maintains, in the realm of cyber offense, the United States remains second-to-none.¹⁶ Washington has long maintained offensive dominance and the Defense Advanced Research Projects Agency (DARPA), the creator of the first packet-switching network, one of the principal precursors to the modern Internet, has recently begun to operate the Pentagon's "Cyber Range," a closed intranet system of sufficient capacity to allow the testing of cyberweapons in order to maintain the United States' offensive edge.¹⁷ Today, the U.S. performs numerous penetrations of foreign networks on a regular basis without being caught.¹⁸ The

Pentagon, Clarke asserts, would likely win a scenario in which the United States' offensive cyber capabilities were pitted against those of the People's Republic in an offensive contest where each state was striving to inflict the greatest damage on targets of defensive parity. Unfortunately, this scenario is unrealistic, as not all cyberdefenses are created equal. In fact, the United States' cyberdefenses are significantly weaker than those of the PRC.

Defensive Capabilities

The leadership of the PRC has developed a strong cyberdefense capacity, which today presents the United States with a considerable obstacle in the event the United States sought to execute cyber attacks upon the People's Republic. China's Internet infrastructure and operational model have evolved in the years since China adopted widespread network integration in a manner fundamentally different from the way in which the Internet grew in the United States. While in the United States the development of software and installation of Internet infrastructure (fiber-optic cable, servers, and routers) has always been the purview of private-sector entities, in the PRC the Internet is a government-run operation. While the leadership of the Chinese Communist Party (CCP) may have originally adopted the state-run Internet model as a means to maintain control over the information transmitted via the web which the PRC's own citizens can view, the party's long years of practice in tightly controlling the Internet have resulted in the establishment of an extremely effective domestic control regime with strong Internet-monitoring, information-control, and internal-defense capacities.¹⁹ As Guobin Yang, the author of a recent book on the political dynamics of the Internet in China, writes, the CCP's censors are constantly evolving and updating their tactics in order to stay one step ahead of China's often-savvy Internet community.²⁰ The government has thus developed a strong internal-defense capacity. Since cyber attacks must ultimately be executed via the networks to which the attacks' physical targets are connected, this internal net-policing force doubles, in effect, as a well-practiced cyberdefense force.

Chinese Internet policymakers have additionally taken the step of assuring that the western-manufactured operating software used by most Chinese citizens and widely used by the government is not compromised. When the CCP agreed to adopt Microsoft's Windows operating system as the primary system used on the mainland, the leadership insisted that Microsoft reveal its proprietary code to the PRC's Internet police so that the software could be altered. Microsoft ultimately agreed to the deal, and the CCP today operates a Windows variant augmented with an encryption module unique to the mainland's software.²¹ The U.S. government, which also uses the Windows system, operates the unaltered software, now widely acknowledged to have been compromised on several occasions.

While these defensive measures are impressive, perhaps the most formidable defensive capability the PRC has developed is the capacity to isolate the mainland's entire network from the global web. In order to maintain control over which sites and information can be accessed by the Chinese populace domestically, the CCP routes all incoming and outgoing Internet traffic through a series of carefully monitored server farms. These Internet gateways can be closed, if required, effectively isolating the mainland's networks from the worldwide web.²² This Internet gateway-control capacity could severely limit an adversary's access to China's networks, significantly degrading the effectiveness of cyber attacks directed at the PRC in the event of a conflict.

Certainly, the United States does not have any comparable defensive capacity. Because both Internet infrastructure and Internet access in the United States are controlled by private-sector Internet Service Providers (ISPs) and their subsidiaries and partners, the

government can only seek to implement and manage network defenses through regulation. As Clarke writes, the list of interests lined up against Internet regulation in the United States is long, and includes a wide range of actors, from information freedom and civil liberties advocates, to software engineering firms and the ISPs themselves.²³ The original concept for the Internet's architecture was developed with free information flow in mind. While the Chinese have managed to impose a relatively effective control regime over the net in the PRC, any such intrusive effort in the United States is likely doomed to failure. This public-private clash of interests explains, in part, the government's anemic progress in establishing stronger Internet defenses despite the evident vulnerability.

In terms of U.S. cyberdefenses, it is useful to think of U.S. networks as being divided into three categories: classified networks, government networks, and the private sector. The "secure" or classified networks include those operated by the intelligence community and the Department of Defense. U.S. Deputy Secretary of Defense William J. Lynn, III, wrote in a recent *Foreign Affairs* article, "Defending a New Domain: The Pentagon's Cyberstrategy," that the DoD has begun the construction of "robust defenses" protecting the Defense Department's own secure network, and plans to expand its defenses to the broader federal government's systems and eventually the private sector.²⁴ In fact, the DoD's own defenses at present are far from robust.

In recent years attacks against the DoD's networks, Lynn admitted, have been rapidly increasing in tempo and effectiveness, and those seeking to break into the network have experienced considerable success. The most widely known attack occurred in 2008, when a flashdrive loaded with malicious code was inserted into a military laptop in the Middle East. The code made its way from the U.S. Central Command's network to the DoD's global network, infiltrating both classified and unclassified systems, establishing, in effect a "digital beachhead" from which the code's foreign-intelligence operators could extract sensitive information. While the source of this particular infiltration is not publicly known, the Defense Department today must be prepared to defend its secure networks against exploitation attempts by more than 100 foreign intelligence organizations.²⁵

The DoD's defensive weaknesses are not limited to the vulnerability of its own networks. Defense personnel, both in theater and stateside, rely upon private-sector defense contractors to perform a number of essential technical and support functions. A cyber adversary, Lynn acknowledges, would not have to beat the DoD's defenses in order to prevent contractors from performing these functions; they would need only defeat the private contractor's own defenses to sever Pentagon-contractor interoperability, an event which would seriously degrade the Pentagon's cyber and kinetic warfighting capacity.²⁶

The Federal Government's cyberdefenses are, at present, also inadequate to the challenge presented by the modern cybersecurity environment. The Government Accountability Office reported in November of 2009 that it had found significant weaknesses in the security of the information systems at 23 of the 24 major executive agencies it audited, proceeding principally from the agencies' failure to adequately implement information security programs.²⁷ The Obama Administration's Comprehensive National Cybersecurity Initiative (CNCI), the White House's ongoing effort to identify and address the key cybersecurity challenges facing the nation today, includes a number of initiatives aimed at strengthening cybersecurity across the .gov domain.²⁸

Finally, the United States' extensive private-sector networks are very poorly defended today. Although both the Department of Homeland Security and U.S. Cyber Command are moving to defend key private-sector networks through partnerships, at present, much of the nation's privately owned critical infrastructure is controlled or automated via networks that

are subject to neither effective regulation mandating security requirements, nor under the charge of any federal cybersecurity organization.

The federal government is now moving to address the nation's vulnerabilities in each of these network categories, but progress remains slow. As Lynn asserts, the DoD is in the process of implementing a fast-track acquisitions process to assure that the Defense Department's networks are protected by the current state-of-the-art in network technologies, and the National Security Agency is developing an active defense system with the capacity to identify and target network intrusions. This active defense concept could have private-sector applications in the near future.²⁹ Additionally, the administration's experts, Department of Homeland Security (DHS), and Cyber Command are working with the private sector to move toward the establishment of better defenses for the United States' extensive network-integrated critical infrastructure.

Cyber Dependence

That network-integrated infrastructure represents a major strategic liability for the United States in the event of a cyber conflict. As former head of the National Security Agency (NSA) and Director of National Intelligence Admiral Mike McConnell has asserted, "... as the most wired nation on Earth [the United States] offers the most targets of significance . . ." to cyber attack.³⁰ No other nation has networked as many critical systems, from the financial system to basic utilities, to military communications and logistics. In many instances, public and private organizations have not only integrated their systems with broader networks, but they have retired the manual backups in order to streamline operations.³¹ The President's "smartgrid" initiative, which proposes the creation of an automated power-metering system to conserve energy, will only create further vulnerabilities to cyber attack should the initiative move forward. In fact, the vast majority of the nation's wired critical infrastructure is privately owned and thus, at present, very poorly protected.

The PRC is not nearly as cyber dependant. In the event of a conflict, the Chinese leadership will be able to operate in the knowledge that much of their critical transportation, power, and sewage infrastructure is either not networked, or has reliable manual backup systems in place.³² Thus cyber dependence turns the United States' overwhelming market advantage in network-enabled efficiency into an exploitable vulnerability in the event of cyber conflict, while the mainland's relative lack of network integration becomes advantageous. The Chinese military is, however, aggressively pursuing the integration of their logistical, communications, and combat operations into a networked system resembling the United States' own system. This pursuit of "informatization," *xinxihua* (信息化), envisions the integration of the entire PLA with a common information system.³³ Thus, the PLA's pursuit of American-style technology-integrated capabilities will likely create targets for cyber attack, significantly increasing the PRC's cyber dependence.

It is the combination of these three factors, cyber offense, cyberdefense, and cyber dependence, as Clarke writes, that must be considered when calculating a nation's comprehensive cyberwar strength. A preponderance of cyber-offensive capability, such as that which the United States commands today, is insufficient to prosecute a cyber conflict if the nation has extensive cyber dependence without the defensive capacity to secure its networked capacities.³⁴ The United States today is in a poor position vis-à-vis the PRC in the event that a cyber conflict should occur. By allowing the emergence of extensive domestic and military cyber exposure without providing a commensurate defense, the United States may already be engaged in self-deterrence in the event of a conflict with any cyber-capable actor, and, at a minimum, is limiting its own coercive options.

Beijing's Intentions

The PRC leadership's intentions in developing China's advanced cyberwarfare capabilities are, in the first place, to deter other nations from pursuing more traditional coercive policies toward the PRC, and in the second, to develop an advanced cyberwarfare capacity that will allow the PRC to asymmetrically challenge any potential adversary in the event of a conflict, regardless of that adversary's conventional strength.

A study conducted by the defense contractor Northrop Grumman for the U.S.-China Economic and Security Review Commission concluded that the PLA's Computer Network Operations (CNO) strategy in the event of a conflict is "... characterized by the combined employment of network warfare tools and electronic warfare weapons against an adversary's information systems in the early phases of a conflict."³⁵ According to two of the PLA's most authoritative documents on military doctrine, the achievement of information dominance "... is one of the key goals for the PLA at the strategic and campaign level." So essential is the seizure of an adversary's information flow that the PLA apparently considers information dominance to be a requirement before moving to achieve air and naval superiority in a local conflict.³⁶

This focus on information dominance is, Admiral McConnell asserts, a specifically anti-American strategy, proceeding from the PLA leadership's assessment that the Chinese military cannot defeat the U.S. military in a conventional scenario, given the United States' technological advantages and extensive experience in prosecuting such conflicts.³⁷

Rather, PLA doctrine advocates the pursuit of asymmetric warfare in order to exploit the weaknesses of a stronger adversary to advantage. Much of what American analysts know of China's asymmetric warfare strategy is contained in a short volume produced by two PLA senior colonels in 1999, *Unrestricted Warfare*. The book offers a detailed blueprint for how conventionally inferior states can defeat status quo powers utilizing nontraditional weapons and tactics. The authors advocate tactics which have come to be known as *shashoujian* (杀手锏), the "assassin's mace," meant to take advantage of weaknesses created by an adversary's apparently superior conventional capabilities. The book calls for "making the weapons to fit the fight," and advocates the manipulation of foreign media, flooding hostile nations with narcotics, controlling markets for natural resources, joining international bodies in order to subvert them, the targeting of civilians if necessary, and the use of cyberwarfare.³⁸

Chinese strategists have devised ways in which the PLA can use its cyberweapons to level the conventional playing field. When military planners on either side of the Pacific imagine likely conflict scenarios between the PRC and the United States, the scenarios inevitably involve PLA units coming into conflict with American naval forces, typically including one or more aircraft carriers, such as the United States employed during the 1996 Taiwan Strait Crisis. Chinese strategists have given considerable attention to the pursuit of defeating U.S. carrier strike groups, including the application of cyberwarfare techniques. In particular, two PLAAF colonels published in 2005 a study enumerating the ways in which cyber and electronic attacks on U.S. vessels at sea could degrade their command, control, communications, computers, and intelligence, surveillance, and reconnaissance (C4ISR) data links to the degree that the vessels would be rendered highly vulnerable to conventional attacks by PLA forces.³⁹ This is one concrete example of the PLA's broad strategy to integrate cyber operations into the military's conventional war-fighting strategies.⁴⁰

While Chinese cyberwarfare doctrine may focus on the integration of cyber capabilities into conventional operations in the event of a conflict, the PRC's cyber capacities are hardly

lying dormant in peacetime. In the last decade the People's Republic has become one of the world's most adept practitioners of cyber espionage.

Cyber Events of Chinese Origin

Chinese cyber espionage experts have been responsible for exfiltrating a staggering amount of data from government agencies, research universities, and private companies in the United States and abroad in the last decade. A list of the PRC's most prominent network penetrations over the last six years follows:⁴¹

2010:

- Google, Inc. revealed that it had been targeted by Chinese hackers seeking to copy its intellectual property and access the Gmail accounts of Chinese dissidents through the application of complex "spear-phishing" techniques.

2009:

- Canadian researchers discovered a highly sophisticated computer program dubbed GhostNet, which had taken over 1,300 computers in over 100 countries, targeting embassies and NGOs working on Tibetan issues.
- U.S. intelligence agencies revealed to the media that Chinese hackers had penetrated the power grid and left behind tools that could later be used to bring down the grid.⁴²
- Germany suffered multiple attacks of Chinese origin, and the PRC denied hacking into the Australian prime minister's computer via email.⁴³
- Chinese hackers targeted South Korean officials via engineered emails.

2008:

- The Indian government confirmed that its Ministry of External Affairs' computer network had been the target of multiple intrusions originating in the PRC.
- The Belgian government reported being targeted by PRC hackers on multiple occasions.
- Chinese intelligence copied the contents of the U.S. Secretary of Commerce's laptop while he was on an official trip to the PRC, and later attempted to use the copied data to hack into Commerce computers.⁴⁴
- Australia, India, and Belgium reported being the target of Chinese hackers.⁴⁵
- The Obama campaign's computers were penetrated by Chinese hackers and a number of draft policy documents were copied.⁴⁶
- Allegations that the White House's computers had been penetrated by Chinese hackers surfaced.
- NASA suffered "massive and sustained" intrusions of Chinese origin.
- The French Embassy Web site was attacked after French politicians met with the Dalai Lama.⁴⁷

2007:

- The governments of Germany, the United Kingdom, and New Zealand each reported being targeted by Chinese hackers.
- United States Nuclear Labs was targeted by malicious emails of Chinese origin.⁴⁸
- MI-5, British domestic intelligence, warned 300 companies in the UK that state-sponsored Chinese hacking was targeting British intellectual property.⁴⁹

2006:

- Chinese hackers targeted the Taiwanese Ministry of Defense.
- The U.S. State Department reported that it was recovering from a Chinese hacking event.
- The U.S. Naval War College's computer infrastructure was attacked by PRC hackers.⁵⁰

2005:

- Several Japanese sites were attacked by Chinese hacktivists.
- Members of the Taiwanese National Security Council were targeted by PRC hackers via socially engineered emails.
- Operation "Titan Rain," ultimately traced back to a server in Guangdong, PRC, resulted in the exfiltration of 10–20 terabytes of data from the Pentagon's unclassified network. Various defense contractors including Lockheed Martin were also targeted.⁵¹

Many of these attacks can be attributed to the PRC with a high degree of confidence, while others can only be tenuously linked to Beijing. These penetrations are not, strictly speaking, cyber attacks, which could potentially merit a conventional response, but in the aggregate they certainly signal that Chinese hackers are engaged in an aggressive campaign of cyber espionage.

As Undersecretary of Defense Lynn reflects, while the theft of industrial and state intellectual property is not an act of war, military strength ultimately relies upon sustained economic vitality. China's apparent effort to level the technological and economic playing field through cyber espionage could severely erode the United States' military effectiveness and economic competitiveness if such espionage continues to proceed unchecked.⁵²

Difficulties of Cyber-Attack Attribution

Cyberwarfare presents strategists and policymakers with a new challenge, the inability to quickly identify the source of an attack. Attack attribution is a requisite before military and elected officials can even begin to contemplate a response, but in a cyberwar, where attacks occur at the speed of light, determining the source of an attack is by no means a certainty. Cyber experts and governments use a number of approaches to mask their cyber espionage activities and would likely use similar methods to conceal the source of their cyber attacks in a conflict scenario.

Attackers may launch their assaults from foreign servers to throw off attempts to trace their work, or may "bounce" their attacks across servers in many nations before striking the intended target. Governments, when accused of ordering cyber assaults or espionage, may blame citizen hacktivists and do nothing, as both the Chinese and Russians do today.

The current state-of-the-art in cyber forensics enables countries and businesses to back-trace attacks, but such operations are often frustrated when the attacker routes his attack through a server hosted in a country or belonging to an interest that will not cooperate with the trace. Even if the trace succeeds in locating the original computer from which the attack was orchestrated, the identity and motivation of the attacker remains a mystery. Forensics may be able to determine that the computer used to create the attacking code was designed with a keyboard arranged for Arabic, Mandarin, or Cyrillic, but such determinations, as Clarke writes, are hardly dispositive as to the identity of the attacker.⁵³

This difficulty in attack attribution has created a distinct “first-mover advantage,” whereby the attacking party may attempt to overwhelm an adversary’s cyberdefenses before the target can identify the source of the attack, or, alternatively, an attacker may seek to deceive the target into believing the attack is being conducted by another actor. Throughout most of the Cold War, attack attribution was not an issue since all parties could identify the source of a missile or bomber relatively quickly, and with considerably more time to craft a response than will be available to American leaders today in the event of a cyber strike.

Policy Recommendations

The United States must seek to improve upon the cyber status quo in a number of areas if the nation’s vulnerabilities are to be addressed and the international cyber environment is to evolve in a manner conducive to shared security. At home, as the authors of a recent study by the Center for Strategic and International Studies urge, the president must declare as a fundamental principle that “. . . cyberspace is a vital asset for the nation and that the United States will protect it using all instruments of national power, in order to ensure national security, public safety, economic prosperity, and the delivery of critical services to the American public.”⁵⁴ Practically, this effort will require the federal government to work with the private sector, both through partnerships and via the creation of effective regulation which will ensure the security of those private entities which own and operate the critical infrastructure upon which we all rely. The legislative process undertaken to create such regulation will be contentious, and the idea of federal regulation of the Internet will be unpopular, but the American people must come to understand that the web is a shared commons upon which we have all come to rely, and that it is a commons under threat.

Technically, cyberdefense may be accomplished through the application of active defense systems, such as that which the NSA is developing today, and through creating incentives for targeted private entities to redevelop un-networked backups which can be relied upon in the event of a network attack. Sensitive networks may have their defenses bolstered through the “closing” or segregating of defense and intelligence systems from the broader web or other alterations to network architecture, which will limit access. The Department of Defense does have a classified cyber doctrine, but no comparable, published, national cyber strategy exists today.⁵⁵ As the authors of a recent National Academy of Sciences study examining American information warfare strategy reflect, today’s “. . . policy and legal framework for guiding and regulating the U.S. use of cyber attack is ill-formed, undeveloped, and highly uncertain.”⁵⁶ While the Obama Administration has signaled its cognizance of the nation’s vulnerability, through such efforts as the release of the Comprehensive National Cybersecurity Initiative, cyberdefense has not received a degree of prioritization commensurate with the critical nature of the issue.

The nation’s leaders must work on the crisis decision-making scenarios in use today to accommodate the emerging realities of the cyber threat. At present, American leaders face the prospect of making critical decisions with limited or deceptive information in extremely truncated timeframes even as undefended domestic infrastructure is coming under attack. The possibility of a poorly calculated or misdirected response under these circumstances is especially alarming in the case of an attack from China, given the PRC’s historical and doctrinal stress upon deception in warfare.⁵⁷

In addition to strengthening both cyberdefenses and policy at home, the United States must lead an international effort to establish a multilateral framework for the adjudication of cybersecurity issues and begin the long process of establishing recognized international norms of cyberwarfare employment. As the authors of the CSIS report reflect, cyberwarfare

is such a recent innovation in international security that there is neither a “lexicon for strategic conflict in cyberspace, nor clear rules of engagement, nor a menu of responses, nor the means to signal intentions to potential opponents.”⁵⁸ During the nuclear era, the policies of deterrence, signaling, and a strategic lexicon took years to work out, and the emergence of the norm of nuclear non-use was by no means a foregone conclusion during the early years of the Cold War. The window of maximum danger during the nuclear era occurred during the early years of American-Soviet nuclear competition, before the “rules of the road” had been established. We are entering a similar window of danger today, with virtually no cyberwarfare norms in place even as many nations are racing to develop cyberwar capabilities. In fact, the only “norm” in use widely today appears to be the conduct of aggressive cyber espionage by all parties with the capability to do so. In many cases, the line between espionage-oriented network penetrations and cyber attack operations is not easily distinguished. The situation at present is thus extremely dangerous.

As well as enlisting a coalition of like-minded nations for the pursuit of a normative approach to cyber security, the United States, as Undersecretary Lynn writes, should strive to establish a global shared warning system for cyberspace application.⁵⁹ The establishment of such a body, although it is likely currently out of the world’s technical reach, could play a critical role in mitigating the dangers of cyber-attack misattribution, and would reinforce the norm of non-offensive use of cyberweapons through objectively publishing detected attacks occurring in violation of an agreed-upon protocol. At present, across the globe, the critical work of shaping nations’ perceptions of cyberwarfare development and use remains purely conceptual.

China is by no means the only potential adversary today with the means to capitalize on the United States’ current cyberwarfare vulnerabilities. If individual states are to be deterred from employing their cyberwarfare capabilities for the purposes of espionage or attack against other nations, the status quo must change in one of two ways, or both. Either cyber-forensic capabilities must improve to such an extent that reliable counterstrike will come to mitigate first-mover advantage and nations will be deterred from attacking due to fear of the consequences and the expectation of international opprobrium, or cyberdefenses must become so robust that states do not anticipate any gain from the prosecution of cyber attack. The United States must prepare itself for both possibilities.

Notes

1. Kevin Anderson, “White House Website Attacked,” *BBC New Online*, May 5, 2001, available at <http://news.bbc.co.uk/2/hi/americas/1313753.stm> (accessed September 2, 2010).
2. Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins Publishers, 2010), 47–53.
3. United States Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2010*, 41–42, available at http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf (accessed September 3, 2010). The figures used are the Pentagon’s estimates of real expenditures, and not those of the official PLA budget.
4. United States Department of Defense, *Annual Report to Congress: The Military Power of the People’s Republic of China 2009*, 27–28, available at http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf (accessed September 3, 2010).
5. Clarke and Knake, *Cyber War*.
6. Ryan Singel, “White House Cyber Czar: ‘There Is No Cyberwar,’” *Wired.com*, March 4, 2010, available at <http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/> (accessed September 2, 2010).

7. *Cyber Threats to National Security*, Symposium Report from The U.S. Naval Institute and CACI International, Inc., July 2010, p. 7, available at http://asymmetrichthreat.net/docs/asymmetric_threat_4_paper.pdf_asia_balance_powers.pdf (accessed September 3, 2010).
8. The U.S.-China Economic and Security Review Commission, *China's Approach to Cyber Operations: Implications for the United States*, Testimony of Larry M. Wortzel before the United States' House of Representatives' Committee on Foreign Affairs, March 10, 2010; and Clarke and Knake, *Cyber War*, 54.
9. The U.S.-China Economic and Security Review Commission, *China's Approach to Cyber Operations*, 3.
10. Clarke and Knake, *Cyber War*, 57–58.
11. United States Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010*, 7.
12. Clarke and Knake, *Cyber War*, 56.
13. For more on the security implications of the global IT supply chain, see *Cyber Threats to National Security*.
14. Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *The Wall Street Journal*, April 8, 2009, available at <http://online.wsj.com/article/SB123914805204099085.html> (accessed September 3, 2010).
15. Clarke and Knake, *Cyber War*, 59.
16. *Ibid.*, 147.
17. William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, vol. 89, no. 5 (September/October 2010): 105.
18. Clarke and Knake, *Cyber War*, 123.
19. Susan Shirk, *China: Fragile Superpower* (New York: Oxford University Press, 2007), 91–93.
20. Guobin Yang, *The Power of the Internet in China: Citizen Activism Online* (New York: Columbia University Press, 2009), 47–51.
21. Clarke and Knake, *Cyber War*, 94.
22. *Ibid.*, 145–148.
23. *Ibid.*, 106–122.
24. Lynn, III, "Defending a New Domain," 98.
25. *Ibid.*, 97–99.
26. *Ibid.*, 104.
27. Government Accountability Office, "Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats," *Statement for the Record to the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate*, GAO-10-230T, November 17, 2009.
28. National Security Council, *The Comprehensive National Cybersecurity Initiative*, available at <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative> (accessed September 6, 2010).
29. Lynn, III, "Defending a New Domain."
30. Mike McConnell, "Mike McConnell on How To Win the Cyber-War We're Losing," *The Washington Post*, February 28, 2010.
31. Clarke and Knake, *Cyber War*, 97.
32. *Ibid.*, 148.
33. United States Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010*, 3.
34. Clarke and Knake, *Cyber War*, 148.
35. Northrop Grumman Corporation, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Prepared for The US-China Economic and Security Review Commission, October 2009, p. 10, available at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (accessed September 7, 2010).

36. Ibid., 11.
37. Clarke and Knake, *Cyber War*, 49.
38. Col. Qiao Liang and Col. Wang Xiangsui, *Unrestricted Warfare* (Panama City, Panama: Pan American Publishing Company, 2002, Trans). Originally published in 1999 by China's People's Liberation Army, Beijing.
39. Larry M. Wortzel, excerpt from *China's Nuclear Forces: Operations, Training, Doctrine, Command, Control and Campaign Planning* (Washington, DC: Strategic Studies Institute, 2007), available at <http://www.strategicstudiesinstitute.army.mil/pubs/print.cfm?q=776> (accessed September 7, 2010).
40. United States Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010*, 37.
41. For a more complete list of Chinese cyber events, see Northrop Grumman Corporation, *Capability of the People's Republic of China*, 67–74.
42. Clarke and Knake, *Cyber War*, 59–60.
43. Northrop Grumman Corporation, *Capability of the People's Republic of China*, 67–74.
44. United States Department of Defense, *Annual Report to Congress: The Military Power of the People's Republic of China 2009*.
45. Northrop Grumman Corporation, *Capability of the People's Republic of China*, 67–74.
46. Clarke and Knake, *Cyber War*, 59–60.
47. Northrop Grumman Corporation, *Capability of the People's Republic of China*, 67–74.
48. Ibid.
49. United States Department of Defense, *Annual Report to Congress: The Military Power of the People's Republic of China 2008*, available at http://www.defense.gov/pubs/pdfs/China_Military_Report_08.pdf (accessed September 8, 2010).
50. Northrop Grumman Corporation, *Capability of the People's Republic of China*, 67–74.
51. Clarke and Knake, *Cyber War*, 58.
52. Lynn, III, "Defending a New Domain," 100.
53. Clarke and Knake, *Cyber War*, 213–215.
54. The Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, p. 5, available at http://ws.infospace.com/cyberdefender_EDC/ws/results/Web/Securing%20Cyberspace%20for%20the%2044th%20Presidency/1/417/TopNavigation/Relevance/iq=true/zoom=off/_iceUrlFlag=7?_iceUrl=true (accessed September 11, 2010).
55. Ibid., 23.
56. National Research Council, National Academy of Sciences, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Executive Summary, p. 4, available at http://www.nap.edu/catalog.php?record_id=12651 (accessed September 17, 2010).
57. United States Department of Defense, *Annual Report to Congress: The Military Power of the People's Republic of China 2009*.
58. The Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency*, 27.
59. Lynn, III, "Defending a New Domain," 104–105.