Threats to Cyberspace and Responses

Recommended Citation

Senior Colonel Fan Gaoyue 作者：樊高月大校, "Threats to Cyberspace and Responses", NAPSNet Special Reports, June 13, 2013, https://nautilus.org/napsnet/napsnet-special-reports/threats-to-cyberspace-and-responses/

by Senior Colonel Fan Gaoyue 作者：樊高月大校

13 June 2013 / 13 日6 月 2013

I. Introduction

For the original Chinese-language version, please go here. In this Special Report Senior Colonel (Retired) Fan Gaoyue argues that the internet and cyberspace in broad terms have an openness and ability to transcend geopolitical borders that makes it vulnerable. Therefore there are several practical measures for international cooperation that can promote cyberspace security.

This work was originally presented at a Swedish-sponsored conference and is being published as a Special Report with the author's permission.

Fan Gaoyue recently retired from the Chinese People's Liberation Army. His most recent assignment was at the Chinese Academy of Military Sciences. He was also a WSD-Handa Fellow at PACFORUM CSIS (Center for Strategic and International Studies) in 2011.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

II. SPECIAL REPORT

Threats to Cyberspace and Responses

Summary: With the advent of information age, internet has become more and more popularized and internet users have increased rapidly to more than 2 billion. On the internet people control traffic and transportation, distribute energy and power, do shopping and pay bill, enjoy music, exchange sentiments and know the world by sending and receiving information. The internet has become the tool to break national borders, communicate global information and exert influence upon international and domestic affairs. However, because of the characteristics that cyberspace exists across the world, transcends geopolitical borders, and is readily accessible in varying degrees to anyone and subject to the availability of the electromagnetic spectrum, cyberspace is seriously threatened by cyber invasions, cybercrimes, computer viruses and worms, network attacks and so on. To deal with these threats, people must raise their consciousness of cyberspace security and strengthen the protection of cyberspace, strengthen the innovation of network technology to reduce the vulnerabilities of network system, establish national cyberspace security watch and warning system to detect and prevent cyber attacks timely and effectively, perfect laws and regulations for cyberspace security to consolidate the management of cyberspace, strengthen international cooperation to promote cyberspace security together.

With the rapid development of computer and network technology, internet era is arriving. At present millions of people live on network technology and more than 2 billion of people carry on routine social communications through internet. On the internet people control traffic and transportation, distribute energy and power, do shopping and pay bill, enjoy music, exchange sentiments and know the world by sending and receiving information. However, network espionage, network fraud, network pornography and computer viruses run rampant, and personal privacy, intellectual property rights and national secrets are seriously threatened while people enjoy all kinds of advantages on the internet. This reality forces us to think and deal with the cyberspace security issues earnestly and seriously.

The roles and characteristics of cyberspace

Cyberspace is composed of hundreds and thousands of interconnected computers, servers, routers, switches, and fiber optic cables and is the nervous system of critical infrastructures such as transportation, energy, telecommunication, public health, banking and finance. With the advent of information age, internet has become more and more popularized and internet users have increased rapidly. From 2000 to 2010, internet users in the world increased from 360 million to more than 2 billion.[i] Till the end of June 2012, the Chinese netizens reached 538 million and the internet penetration rate reached 39.9 %; mobile phone netizens reached 388 million, network shoppers reached 210 million, network bank users reached 191 million, with an increase about 9.2%, 8.2% and 14.8% respectively compared with the previous year; the total domain names in China is 8.73 million (including 3.98 million .CN domain names) and the total websites increased to 2.5 million.[ii] Every day countless netizens obtain or send information on the internet all the time all over the world. The internet has become an effective tool to break national borders, communicate global information and exert influence upon international and domestic affairs. The wide application of various networks has greatly raised the efficiency of social labor and production, reduced cost and changed the approaches of activities and decisions by enterprises, governments and social entities. The public and specialized information fast flowing on the international networks, regional networks or city networks has already become the motive force to promote the rapid development of politics, economy, military affairs and diplomacy in the world.

Networks now develop very fast and become increasingly popular. It is of great importance to recognize the basic characteristics of cyberspace in running and applying networks. According to the development and application of networks, cyberspace is mainly characterized by: (1)Created, maintained, owned, and operated by public, private and government stakeholders and exists across the globe; (2) Changes as technology, architectures, processes and expertise co-evolve to produce new capabilities and operating constructs; (3) Subject to the availability of the electromagnetic spectrum; (4) Allows high rates of operational maneuver that capitalizes on decision-quality information moving at speeds that approach the speed of light; (5) Enables operations across the domains of air, land , maritime and space; (6) Transcends commonly defined geopolitical borders; (7) Formed by supporting critical infrastructure, devices that store, process and transmit data, the use of software and hardware applications; (8) Includes data, voice, and video “at rest” and “in motion”; (9) readily accessible in varying degrees to other nations, organizations, partners, the private sector and adversaries. [iii]Besides, there are vulnerabilities in cyberspace architecture, network technology, physical protection, open source information, personnel training and cyberspace policy.

The serious threats to cyberspace

Owing to the basic characteristics and vulnerabilities described above, cyberspace is facing a variety of complicated and dangerous threats. Some threats come from abroad, some from homeland, some from national governments, some from non-state actors, and still some from the vulnerabilities of computer systems. Small technology may give rise to big impact. The potential adversary who can not make complicated and expensive weapon systems may produce obvious impact upon a big country’s security through networks. Ninety percent of the participants in 2003 Computer Security Institute survey reported using antivirus software on their network systems, yet 85 percent of their systems had been damaged by computer viruses. In the same survey, 89 percent of the respondents had installed computer firewalls, and 60 percent had intrusion detection systems. Nevertheless, 90 percent reported that security breaches had taken place, and 40 percent of their systems had been penetrated from outside their networks.[iv] The threats to cyberspace can be classified into five categories:

1. Cyber invasion. Cyber invasion is referred to the intrusion into networks to collect information, but neither add or modify data nor undermine or interfere with the networks. Both government intelligence departments and non-state actors emphasize to obtain information from networks because it is much easier and cheaper to get information from networks than human intelligence. Hence cyber invasions increase rapidly. In August 2005, IBM Global Services issued *IBM Security Report: Government, Financial Services and Manufacturing Sector Top Targets of Security Attacks in First Half of 2005*, saying that the first half of that year the reported invasions in the world reached 237 million, among which governmental organizations suffered most, reaching 54 million; manufacturing sectors ranked second, reaching 36 million; financial services and health services ranked third and fourth, reaching 34 million and 17 million respectively. By country, the United States government and sectors concerned suffered most, reaching 12 million; New Zealand ranked second, reaching 1.2 million; China ranked third, reaching 1 million.[v] *China Internet Security Posture 2011* shows that about 47 thousand IP addresses abroad (22.8 % in Japan, 20.4 % in the United States, 7.1 % in South Korea) participated in controlling about 8.9 million main servers within China; 11,851 IP addresses abroad executed remote control of 10,593 websites within China by Trojan programs.[vi] From January to March 2012, IP addresses revealed that both the Net Station of the Defense Ministry of the People's Republic of China and China Military Net Station suffered 80,000 invasions from abroad monthly.[vii] These cyber invasions, either for getting money, obtaining intellectual property rights or undermining important defense systems, constitute complicated and austere challenges to a country's politics, economy, military affairs and diplomacy.

2. Cybercrime. Cybercrime is referred to the use of networks to carry out criminal activities such as running pornography net station, engaging in computer-related fraud and selling illegal products by networks. The Federal Bureau of Investigation of the United States investigated 547 criminal cases and ended 399 of them in 1998, and investigated 1154 criminal cases and ended 912 of them in 1999, with the quantity of criminal cases doubled in a year. Since 2006 the total quantity of cybercrime on China's networks has also run high all the time, with an annual average at about 4.7 million. In fact the actual occurrence of cybercrime doubles this number according to the most conservative estimate of some professionals. Among the cybercrimes the most prominent problem is pornographic materials which endanger the health and mentality of the under-aged gravely. The copyrights of software, video works and records are seriously infringed by pirate activities, which have caused enormous losses to the owners. Cyber business is often harassed by frauds: some credit cards are embezzled; some never see the merchandise they bought; some delivered goods but never got the payment for goods. According the statistics from Japan and Taiwan, pornography cases occupy 30~35 percent of cybercrimes; cyber fraud, sale of illegal products, intimidation and blackmail, insult and slander also occupy a bigger percentage compared with other criminal offences.

3. Malware. Malware usually includes computer virus and worm, Trojan horse and logic bomb, spam and phishing. Computer virus and worm are referred to the use of illegal channels in network to transmit programs to undermine computer and its systems. Computer virus and worm emerged and spread widely in 1980s. The most noted worms and viruses include: *Morris Worm*, which resulted in more than 6 thousand systems infected, occupying one-tenth internets at that time; *Melissa Virus*, which infected more than 100,000 main servers within 4 days; *Red Code Virus*, which influenced 150,000 computers within 14 hours; *Nimda*, which spread to the whole country within one hour and attacked 86,000 computers in a few days by combining computer worm and virus together; *Stuxnet*, which was employed to attack Iran's nuclear facilities and was regarded as a new chapter in making use of cyberspace because of its complicated techniques and excellent pertinence.[viii] Trojan horse and logic bomb are subversive codes attached in programs or systems and begin to sabotage under given conditions. Spam is the junk mails sent to computer users by business man to promote sales and only can cause tiny trouble. Phishing is to trick

computer users into giving their account numbers and passwords by inducing them into entering seemingly legal homepage and becomes one of the most prevalent methods to cheat in networks. These malwares usually undermine computer systems by way of leak invasion, backdoor embedding, hardware infusion or input-path introduction.

4. Cyber attack. So far a real "cyber war" has never occurred but cyber attacks happened several times and achieved brilliant victory. In March 2003, the U.S. forces intruded into the Iraq military's classified network and sent emails to thousands of Iraq officers persuading them to line up their tanks and armored vehicles outside of their military bases and leave to save their lives, which resulted in the disappearance of the Iraq troops without fight. On the deep night of September 6, 2007, the Israel fighters cheated Syria's air defense system by cyber attack and destroyed the "nuclear facilities" within Syria without any loss. During the Russia- Georgia conflict broken out on August 7, 2008, Russia launched continuous, complicated and intensive cyber attacks upon Georgia, resulting in that Georgia lost control of its domain name ".ge" and was obliged to transfer its governmental net stations to foreign servers, but Russia changed its attack paths pretending that the cyber attacks were from Georgia, which triggered the automatic protection system of most foreign banks to shut up their linkage with Georgian banks so that the Georgian banks' business collapsed because of being unable to visit European balancing systems. As a result, the Georgian credit card system ceased to work and mobile phone system broke down as well.[ix] Although cyber war has never occurred until now, the threat of cyber war exists indeed. Some country began to train cyber warrior in 1990s and has now built large cyberspace operation forces, Service cyberspace command and joint cyberspace command, which often conduct cyberspace operation exercises and can wage a cyber war once there is a need.
5. Cyber vulnerabilities. The fragility of computer system security, or the capability in software and hardware to enter into network without authorization, increased evidently from 2000 to 2002, with the number of vulnerabilities increasing from 1090 to 4129. Even if the software and hardware are integrated into a set of application system, they are still in the danger of being juggled. Most of the information technology products used by some countries are manufactured and assembled by foreign countries. It is doubtful whether these products themselves bear unpredictable risk.[x] China is short of core computer technology (chips) with its own property rights and most of its computers adopt foreign core technology, which buries hidden trouble for its cyber security. Therefore new fragility of computer system security will appear all the time. To guarantee the security of network and system, we must persistently upgrade protection measures instead of relying on the security protection means available.
6. Besides these manmade threats, cyberspace still faces some natural and accidental threats. Natural threats that can damage and disrupt cyberspace include acts of nature such as floods, hurricanes, solar flares, lightning and tornados. Accidental threats are unpredictable and can take many forms, including a backhoe cutting a fiber optic cable of a key cyberspace node, inadvertent introduction of viruses, and so on.

Responses to the threats

In information age cyberspace has already become the base of all kinds of social activities and provided important support for national politics, economy, military affairs, diplomacy, civil infrastructure and national security. If cyberspace suffers heavy attacks, the country's energy and power, traffic and transportation, finance and other sectors will suffer enormously, which in turn will greatly affect social stability and national security. Hence practical and effective measures must be taken to ensure national cyberspace security.

First, launch national cyber security education movement to raise self-consciousness for cyber

security protection. Cyber threats cannot be seen or touched, coming and leaving without footprints and it is hard to feel their existence. Therefore the cyber security awareness of most netizens is rather weak. At present most countries are eager to build network at large scale and with high speed, neglecting related security support measures. A lot of application systems are actually in the state of being non-defensive, leaving enormous hidden trouble for cyberspace security. Government and sectors concerned should finance national cyberspace security education to make all the netizens to understand the grave threats they face and the enormous damage they might suffer by radio, television, internet, newspaper and magazine. Thus the cyberspace security awareness of netizens can be strengthened and the protection of networked systems can be consolidated.

Second, strengthen network technology innovation to reduce vulnerabilities of networked systems. Cyber attacks can burst onto a nation's networks with little or no warning and spread so fast that many victims never have a chance to hear the alarms. Even with forewarning, they likely would not have had the time, knowledge, or tools needed to protect themselves. Therefore organizations that rely on networked systems must take the following proactive steps to identify and remedy their vulnerabilities, rather than waiting for an attacker to be stopped or until alerted of an impending attack. (1) Persistently assess the vulnerabilities of networked systems and adopt timely remediation measures. (2) Create a multilayered defense and a resilient network to remedy the most serious vulnerabilities. (3) Invest in research and development of new network protection products to reduce the vulnerabilities of networked systems. (4) Often conduct cyber security protection exercises to ensure networks against being attacked or be able to restore functions in short time after being attacked so as to reduce the damages of cyber attacks.

Third, establish national cyberspace security response system to detect and prevent cyber attacks timely. The vast majority of a country's cyberspace is usually not owned by any public or private group and there is no panoramic vantage point from which we can see attacks coming or spreading. To mitigate the impact of cyber attacks, information about them must disseminate widely and quickly. Analytical and incident response capabilities that exist in numerous organizations should be coordinated to determine how to best defend against an attack, mitigate effects, and restore service. Therefore, a national cyberspace security response system should be set up by governmental and nongovernmental entities to be responsible for analyzing, warning and managing incidents of national significance; promoting continuity in government systems and private sector infrastructures; and increasing information sharing across and between organizations to improve cyberspace security. The system should include organizations such as information sharing and analysis center, incident operations center, incident management center, response contingency center, and coordinate with governmental organizations such as national communication system, national infrastructure protection center and national energy support department to bring national cyberspace security watch-and-warning work into full play. Thus, we can timely detect potentially damaging activity in cyberspace, analyze harms and warn potential victims, coordinate incident responses, and restore essential services that have been damaged.

Fourth, perfect cyberspace laws and regulations to strengthen cyberspace management. Nowadays there are more than 4 billion wireless digital equipment in the world; one-third population use internet; countless people also have contacts with internet in their daily lives. Many countries have made cyberspace laws and regulations to strengthen cyberspace management and safeguard cyberspace security. For example, China has successively established laws and regulations such as *Regulations of the People's Republic of China for Computer and Information Systems Security Protection*, *Provisional Rules of the People's Republic of China for management of Computer and Information Network and International Internet*, and *Measures for Computer and Information Network and International Internet Security Protection Management*. Besides, 30 countries including 26 member States of the Council of Europe, the United States, Canada, Japan and South

Africa, signed *Convention on Cybercrime* in Budapest in November 2001, hoping to work together to promote cyberspace security. These international and domestic laws and regulations have played important roles in strengthening cyberspace management and safeguarding cyberspace security. However, these laws and regulations can no longer entirely satisfy the requirements of the rapid development of various networks. They need to be perfected on the one hand and new laws and regulations need to be made on the other. To manage network more effectively to assure cyberspace security, we need to do the following: (1) Revise out-of-date cyberspace security laws and regulations to enrich their contents and make them more practical; (2) Make new cyberspace security laws and regulations to cover the domains that are not involved such as the establishment of identity management (Identity management is not just about authenticating people. Authentication mechanisms also can help ensure that online transactions only involve trustworthy data, hardware and software for networks and devices.) (3) Strengthen law enforcement to raise the level of cyberspace security management.

Fifth, strengthen international cooperation to promote cyberspace security. As the cyberspace of one country is closely interconnected with international cyberspace and is dissimilar to the traditional territorial land, sea and air which have definite national boundary, it is far from enough to rely on one's own effort to safeguard one's own cyberspace security. Therefore we should do the following to strengthen international cooperation and promote cyberspace security together. (1) Enlarge signatories to *Convention on Cybercrime* so as to deal with together cybercrimes such as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to infringements of copyright and related rights. (2) Promote to establish international "watch-and-warning" network system to detect and prevent cyber attacks that are coming and spreading in time. (3) Build international law enforcement cooperation mechanisms to strike cybercrimes together and enhance the intensity of striking transnational cybercrimes. (4) Hold international conferences on cyber security regularly or irregularly to discuss the ways and methods to cope with threats and challenges to cyberspace security. (5) Establish international behavior norms to safeguard cyberspace security as soon as possible and follow these norms together to contribute to the realization of international cyberspace security. (6) Negotiate and sign an agreement or treaty to prevent cyber war as soon as possible to draw a clear line for cyber war and forbid attacks on national economy and people's livelihood network systems such as power supply, water supply, finance, medical care, education, and prevent to escalate ordinary cyber attacks into a cyber war to ensure that the information environment upon which people rely to live will not suffer ruinous strike.

The views expressed here are solely that of the author and do not stand for the views of PLA Academy of Military Science.

III. NAUTILUS INVITES YOUR RESPONSES

The Nautilus Peace and Security Network invites your responses to this report. Please leave a comment below or send your response to: nautilus@nautilus.org. Comments will only be posted if they include the author's name and affiliation.

IV. REFERENCES

[i] Department of Defense, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, July 2011.

[ii]China Internet Information Center, CHINA INTERNET DEVELOPMENT POSTURE REPORT, July 2012.

[iii] C JC S, THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS, p.3, December 2006.

[iv] The White House, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, P. 8, February 2003.

[v] IBM Global Services, IBM SECURITY REPORT: GOVERNMENT, FINANCIAL SERVICES AND MANUFACTURING SECTORS TOP TARGETS OF SECURITY ATTACKS IN FIRST HALF OF 2005, August 2, 2005.

[vi] Yang Tintin and Wu Duoke, NETWORK ATTACKS ON CHINA INCREASE ENORMOUSLY, Global Times, March 21, 2012.

[vii] Liu Yang, DEPARTMENT OF NATIONAL DEFENSE: CHINA'S MILITARY WEBSITES SUFFERED EIGHTY THOUSAND ATTACKS FROM ABROAD, Global Times, March 30, 2012.

[viii] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, ON CYBER WARFARE, A CHATHAM HOUSE REPORT, 2010, P.7.

[ix] Richard A. Clarke and Robert K. Knake, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT, Harper Collins Publishers, 2010.

[x] The White House, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, P. 8, February 2003.

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/threats-to-cyberspac--and-responses/

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org