Reflection of the Nation Cybersecurity's Evolution

ZHENG An-ka
Academy of Xi'an Communication
Department of Communication Command
Xi'an,China
akzheng@126.com

Song Ping
Academy of Xi'an Communication
Department of Communication Command
Xi'an,China
songping_s@126.com

HAN Bing-xia
Academy of Xi'an Communication
Department of Communication Command
Xi'an,China
hanbinxia1@163.com

ZHENG Min-jiao
Academy of Xi'an Communication
Department of Information Security
Xi'an,China
mjzzheng@gmail.com

Abstract—**Cybersecurity, as stated in the 2010 National Security Strategy of America, "threats represent one of the most serious national security, public safety, and economic challenges we face as a nation". This paper examines the cybersecurity situation that the nation faces. Based on this, the vulnerabilities present in information systems and systems supporting critical infrastructure to cyberattacks are discussed. The argument is presented that China's internet censorship techniques have improved that nation's Cybersecurity, which could affect the outcome of a conflict in cyberspace. The key future features of the Cybersecurity in China are put forth at the end of the treatise. The author believes such analysis can credibly help the establishment of the national Cybersecurity strategy.**

Keywords-cybersecurity; cyberthreats; cyberattack; cyberspace

I. INTRODUCTION

Nearly every aspect of contemporary society increasingly depends upon information technology systems and networks. This includes increasing computer interconnectivity, particularly through the widespread use of the Internet as a medium of communication and commerce. While providing significant benefits, this increased interconnectivity can also create vulnerabilities to cyber-based threats. "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare…it has become just as critical to military operations as land, sea, air, and space." These words, written by Deputy Secretary of Defense William Lynn last fall in Foreign Affairs, cemented the status of cyberspace as a domain of warfare like all others.

The nation faces an evolving array of cyber-based threats arising from a variety of sources. Sources of threats include criminal groups, hackers, terrorists, organization insiders, and foreign nations engaged in crime, political activism, or espionage and information warfare. The nature of cyber attacks can vastly enhance their reach and impact due to the fact that attackers do not need to be physically close to their victims and can more easily remain anonymous, among other things. The magnitude of the threat is compounded by the ever-increasing sophistication of cyber attack techniques, such as attacks that may combine multiple techniques. Using these techniques, threat actors may target individuals, businesses, critical infrastructures, or government organizations.

Consequently, the security of cyberspace is essential to protecting national and economic security, public health and safety, and the flow of commerce. Conversely, ineffective information security controls can result in significant risks, including: (1) loss or theft of resources, such as federal payments and collections; (2) inappropriate access to and disclosure, modification, or destruction of sensitive information, such as national security information, personal taxpayer information, or proprietary business information; (3) disruption of critical operations supporting critical infrastructure, national defense, or emergency services; (4) undermining of agency missions due to embarrassing incidents that erode the public's confidence in government; (5) and use of computer resources for unauthorized purposes or to launch attacks on other computers systems.

II. CYBERSECURITY SITUATION OF THE NATION

Deterrence in cyberspace, as with other domains, relies on two principal mechanisms: denying an adversary's objectives and, if necessary, imposing costs on an adversary for aggression. Cyber-based threats are evolving and growing and arise from a wide array of sources. These threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Table 1 shows common sources of cyber threats.

TABLE I. SOURCES OF CYBERSECURITY THREATS

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud,

	and computer extortion. International corporate spies and criminal organizations also pose a threat to the Country through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

These sources of cyber threats make use of various techniques, or exploits, that may adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. Table 2 provides descriptions of common types of cyber exploits.

TABLE II. THREATS TYPES OF CYBER EXPLOITS

Type of exploit	**Description**
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Logic bombs	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured Query Language (SQL) injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer– sometimes with a powerful antenna–searching for unsecured wireless networks.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

III. VULNERABILITY OF INFORMATION SYSTEM AND CRITICAL INFRASTRUCTURE TO CYBER ATTACKS

Significant weaknesses in information security controls continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. For example, agency, inspectors general, and GAO assessments of information security controls during fiscal year 2011 revealed that most major federal agencies had weaknesses in most of the five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which helps avoid significant disruptions in computer-dependent operations; and (5) agencywide information security programs, which provide a framework for ensuring that risks are understood and that effective controls are selected and implemented. Figure 1 shows the number of agencies that had vulnerabilities in these five information security control categories.

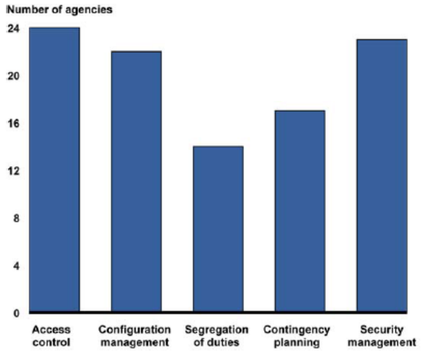

Figure 1. Information Security Weaknesses at 24 Major Federal Agencies in 2011

In addition, securing the control systems that monitor and control sensitive processes and physical functions supporting many of our nation's critical infrastructures is a national priority, and we have identified vulnerabilities in these systems. For example, the critical infrastructure control systems faced increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of possible attacks. Specifically, the critical infrastructure owners faced both technical and organizational challenges to securing control systems, such as limited processing capabilities and developing compelling business cases for investing in control systems security, among others.

We made recommendations to the department of national security to develop a strategy for coordinating control systems security efforts and enhance information sharing with relevant stakeholders; found industrial control systems cyber emergency response organization to provide industrial control system stakeholders with situational awareness and analytical support to effectively manage risk. In addition, it has taken several actions, such as developing a catalog of recommended security practices for control systems, developing a cybersecurity evaluation tool that allows asset owners to assess their control systems and overall security posture, and collaborating with others to promote control standards and system security. We have not evaluated these activities to assess their effectiveness in improving the security of control systems against cyber threats.

In addition to those present in information systems and systems supporting critical infrastructure, vulnerabilities in mobile computing devices used by individuals or organizations may provide openings to cyber threats. For example, consumers and information agencies are increasing their use of mobile devices to communicate and access services over the Internet. The use of these devices offers many benefits including ease of sending and checking messages and remotely accessing information online; however, it can also introduce information security risks if not properly protected. We have ongoing work to determine (1) what common security threats and vulnerabilities affect generally available cellphones, smartphones, and tablets; (2) what security features and practices have been identified to mitigate the risks associated with these vulnerabilities; and (3) the extent to which government and private entities are addressing security vulnerabilities of mobile devices.

IV. Internet censorship in our nation

For the purposes of this analysis, "internet censorship" is any measure enacted to restrict internet accessibility, processes, functions, or content based on sociopolitical imperatives. Such efforts take place in four distinct realms: laws and regulations; norms; markets; and architecture. This paper emphasizes the architectural component, which has the most direct implications for situational awareness. The term "architecture" refers to the physical dimension of cyberspace, described in the National Military Strategy for Cyberspace Operations as "information systems and networks, computers and communications systems, and supporting infrastructures." Architecture also encompasses network design and layout and the nature of connections with other networks, including those beyond national borders.

States can conduct censorship at four key architectural layers. These include, from least to most centralized: individual computers, organizations, internet service providers (ISPs), and the internet backbone. Our nation has generally succeeded in exerting control at each of these four layers.

V. Key future features of Cybersecurity

An analysis of some of the key future features of Cybersecurity domain in our country can inform our understanding of the cybersecurity situational awareness prospects. Two features in particular—international gateways and filtering capabilities—bear closer examination.

A. International Gateways

The overwhelming majority of China's internet communications with the outside world transit just three international gateways located in Beijing in the north, Shanghai in the east, and Guangzhou in the south. By design, this centralization of international internet connections allows government to exert a significant level of control over data traversing China's national-level networks. As a result, according to an account by journalist James Fallows, Chinese authorities can: physically monitor all internet traffic into or out of the country. They do so by installing at each of these few "international gateways" a device called a "tapper" or "network sniffer," which can mirror every packet of data going in or out…. "Mirroring" is the term for normal copying or backup operations, and in this case real though extremely small mirrors are employed. Information travels along fiber-optic cables as little pulses of light, and as these travel through the Chinese gateway routers, numerous tiny mirrors bounce reflections of them to a separate set of… computers.

B. Filtering Capabilities

This separate set of computers, known colloquially as "Great Firewall," allows authentic institution to surveil and filter internet traffic. The system leverages a set of mechanisms to evaluate and analyze the safety of network data. Future cyber filtering capabilities should be non-intrusion detection systems. Those systems employ deep packet inspection (DPI), described as the ability "to look within the application payload of a packet or traffic stream and make decisions on the significance of that data based on the content of that data" (emphasis original). This is opposed to less sophisticated utilities that only analyze data labels, such as packet headers, which contain important but less specific information like data origin and destination.An important caveat here is that DPI technology is generally effective only on data sent "in the clear," or in unencrypted form. This weakness allows users to leverage virtual private networks (VPN) to "scale" the Great Firewall.

C. Enhanced Cybersecurity Services

As an additional and optional part of the program, the Government will furnish classified threat and technical information to voluntarily participating their Commercial Service Providers (CSPs). This sensitive Government furnished information enables the CSPs on behalf of their customers, to counter additional types of known malicious activity and to further protect various departments' program information. Any CSPs that are capable of implementing the Government furnished information in compliance with security requirements are eligible to participate and offer the cybersecurity services to participating companies. CSPs may also charge for providing this service to participating companies.

VI. CONCLUSION

In summary, the cyber-threats facing the nation are evolving and growing, with a wide array of potential threat actors having access to increasingly sophisticated techniques for exploiting system vulnerabilities. The danger posed by these threats is heightened by the weaknesses that continue to exist in information systems and systems supporting critical infrastructures. Ensuring the security of these systems is critical to avoiding potentially devastating impacts, including loss, disclosure, or modification of personal or sensitive information; disruption or destruction of critical infrastructure; and damage to our national and economic security. We should: Recognize and adapt to the military's increasing need for reliable and secure networks; Build and enhance existing military alliances to confront potential threats in cyberspace; Expand cyberspace cooperation with allies and partners to increase collective security.

REFERENCES

[1] United States Government Accountability Office, Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure, GAO-11-865T, Washington, D.C., July 2011.

[2] United States Government Accountability Office, Cybersecurity: Threats Impacting the Nation, GAO-12-666T. Washington, D.C., April 2012.

[3] Office of the President of the United States, Department of Defense Strategy for Operating in Cybersapce, D20110714, Washington, D.C., July 2011.

[4] David A. Gale, Maj, USAF, "Cybermad: Should the United States Adopt a Mutually Assured Destruction Policy for Cyberspace?" Maxwell Air Force Base, Alabama, April 2009.

[5] Barnes, Julian E, "Cyber-attack on Defense Department Computers Raises Concerns." Los Angeles Times, Nov. 2008.

[6] Department of Defense, FACT SHEET: Defense Industrial Base (DIB) Cybersecurity Activities, May 2012.

[7] General Keith Alexander. "House Armed Services Subcommittee, Cyberspace Operations Testimony." Washington D.C., Sept. 2010.