Strategic Study of CAE 2021 Vol. 23 No.2
DOI 10.15302/J-SSCAE-2021.02.001

Construction of Strategic Early-Warning System in Cyberspace

Zhuang Honglin, Yao Le, Wang Sheng, Gu Jiaxiang, Wu Ye, Xie Kai

National Key Laboratory of Science and Technology on Information System Security, Beijing 100191, China

Abstract: Strategic early warnings in cyberspace refer to a monitoring and warning system that is established by a country or group for early detection, tracking, identification, and notification of incoming major cyberattacks or the spread of powerful malicious software. This is an important component of the national security defense system. The implementation of a national cyber development strategy in China requires the construction of a strategic early-warning system for cyberspace. This study analyzes the major characteristics and basic requirements for such a system. Four types of warnings are studied: security vulnerabilities, security threats, intrusion attacks, and abnormal behavior warnings. We review existing strategic early-warning and monitoring systems for cyberspace in China and abroad. As a result, four key projects are emphasized: (1) cyberspace surveying and mapping systems, (2) vulnerability collection and early-warning platforms, (3) threat intelligence perception and push systems, and (4) security monitoring and comprehensive early-warning systems. Finally, we propose several countermeasures and suggestions to promote the strategic early-warning system in cyberspace, including (1) strengthening high-level coordination, (2) focusing on data integration from multiple sources, (3) establishing professional early-warning agencies, (4) conducting regular security assessments, and (5) implementing a grading mechanism for threats and early warnings.

Keywords: cyberspace security; strategic early warning; situation awareness; system construction

1 Introduction

Strategic early warnings refer to a comprehensive vigilance method, in which a country uses an early-warning technology to detect and monitor the activities of strategic offensive weapons by hostile forces. Early warnings can defend against sudden attacks to guarantee national security. Cyberspace has become the fifth largest space in the world (after land, sea, air, and space). As a pillar of economic and social development, cyberspace is now a field of national security. Strengthening situational awareness related to cyberspace, enhancing strategic early-warning capabilities, and ensuring the security of network boundaries are major problems for national security.

Previous studies on early warnings for cybersecurity proposed the early-warning method based on the statistical law of intrusion events [1], strategic intelligence assurance based on decision demand [2], and situational awareness based on data fusion [3]. These research results improved the construction of cyberspace situational awareness and early-warning security systems from different perspectives. Moreover, the United States has established a strategic early-warning system for cyberspace based on big data. Their system obtains intelligence by monitoring global network communication data, obtaining server data from major domestic enterprises, sharing data between departments and various allies, etc., to provide early warnings for network security and the integrity of system links [4].

To respond to the increasingly complex security situation in cyberspace and effectively resist large-scale

Received date: February 05, 2021**; Revised date:** March 07, 2021

Corresponding author: Zhuang Honglin, researcher of National Key Laboratory of Science and Technology on Information System Security. Major research field is cyberspace security. E-mail: zhlxsjl@163.com

Funding program: CAE Advisory Project “Network Power” (2020-ZD-14)

Chinese version: Strategic Study of CAE 2021, 23(1): 001–007

Cited item: Zhuang Honglin et al. Construction of Strategic Early-Warning System in Cyberspace. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2021.01.001

national cyberattacks, it is essential to build and improve strategic early-warning systems in cyberspace. Based on theoretical analysis and current situation research, this study proposes key concepts and countermeasures for the establishment of a strategic early-warning system in cyberspace. Such a system should address the following challenges: (1) incomplete control of network assets, (2) difficulty in sharing security-monitoring data, and (3) difficulty in obtaining evidence for cyberattacks.

2 Concept, characteristics, and application value of strategic early warnings in cyberspace

2.1 Basic concepts of strategic early warnings in cyberspace

According to the traditional definition, a strategic early warning refers to measures taken to detect, track, and identify incoming long-range ballistic missiles, strategic bombers, cruise missiles, and other strategic weapons early, and to issue timely warnings. The mission is to detect the incoming target and its various parameters as soon as possible, process the information obtained, track and identify the incoming target, and provide real-time information for military decision-making, strategic weapon use, civil defense preparations, etc. [5].

Cyberspace is a virtual space that differs from physical spaces (e.g., land, sea, air, and space). Cyberattacks have an immediate effect and replicate quickly. Thus, cyberspace defense systems should be focused on major cyberattacks launched by national-level hackers and the spread of powerful malicious software. Using the traditional definition of strategic early warnings for reference, we can define its cyberspace version as a monitoring and warning system established by a country or group for early detection, tracking, identification, and notification of incoming major cyberattacks or the spread of powerful malicious software [6]. Such a system is an important part of the national defense system.

2.2 Characteristics of strategic early warnings in cyberspace

Cyberspace attacks and defenses have a unique mechanism compared with confrontations in physical space. Therefore, national strategic early warnings would be significantly different for cyberspace and physical space. Effective implementation of a strategic early-warning system requires a deep understanding of the mechanism and characteristics of cyberspace confrontations.

2.2.1 Government should be responsible for early warnings

External defense systems should protect against threats on land, sea, air, and space. The boundaries of the physical space are clear. The national defense forces are responsible for strategic early warnings, and the most significant threats are strategic weapons in air and space [7]. Similarly, the Internet and telecommunications networks are the main entities of cyberspace, and the corresponding management is mainly handled by government departments. According to the principle “the management is responsible,” the government should be the main entity responsible for strategic early warnings in cyberspace.

2.2.2 Wider range of early warnings and precautions

Cyberattacks can be launched from outside or inside. It may be the action of a country, an illegal organization, or an individual. The adversaries in physical space are mainly hostile national forces. By contrast, the adversaries in cyberspace include not only national-level advanced persistent threat organizations and terrorist forces but also civil hacker organizations and insiders. Therefore, the range of threats is broader and more complex.

2.2.3 Shorter warning time

In cyberspace, a target is attacked directly with an immediate effect. Network interoperability and the replication and spread of viruses in a network attack result in the scenario “one machine is infected, multiple machines are infected, and the area is paralyzed.” Moreover, viruses spread rapidly across networks and affect other networks. Compared with physical space wherein strategic attacks usually consider multiple factors to start a war, cyberspace has a low attack threshold; the attack time is random and short. Moreover, it may be attacked by hostile forces and hackers any time. Therefore, early warnings should be timely.

2.2.4 Early-warning targets are highly dynamic

Network technology continuously evolves. Thus, methods of cyberattacks are continuously adjusted and upgraded in response to changes in network characteristics and updates of technical facilities. Offensive and defensive methods evolve and compete in the game of cyberattacks, showing a trend of declining and advancing

DOI 10.15302/J-SSCAE-2021.02.001

each other. Moreover, the effect of specific cyberattacks dynamically changes, which poses a challenge to strategic assessments.

2.2.5 Strategic judgment is related to the attributes of defense objects

The strategic nature of physical space weapons (e.g., long-range ballistic missiles, strategic bombers, and cruise missiles) is easy to define and has been unanimously recognized internationally. Cyberattack weapons are highly specific, and their attack effects are closely related to the attacked party's network structure, attributes, software and hardware systems, and defense mechanisms, which are difficult to determine. Therefore, when we evaluate whether a cyberattack method is strategic, we need to combine the network attributes of the attacked object. Only cyberattack methods that match and achieve strategic threats should be listed as key warning targets.

2.3 Application value of strategic early warnings in cyberspace

Cyberspace confrontation has the following characteristics: high technological level, multiple targets, complex elements, time sensitivity, ambiguity, and considerable data. It has important strategic significance for scientific decision-making in cyber defense operations, winning initiatives, and promoting the modernization of network governance capabilities to build a strategic early-warning system in cyberspace. Such a system should have the following key capabilities: a comprehensive grasp of network software and hardware assets, in-depth mining of information security vulnerabilities, extensive acquisition of network attack methods and behavior characteristics, real-time monitoring of network threats, effective monitoring and aggregation of abnormal behaviors, analysis and discovery of the internal relationship of security incidents, and comprehensive research and audit of the network security.

Strategic early warnings are essential for handling major cybersecurity incidents rapidly and effectively. Constructing the basic information database of network assets, and investigating and mastering the security vulnerabilities of information systems are required for strategic early warnings in cyberspace. Maps are an important tool for people to perceive the environment. Virtual cyberspace also requires a "cyberspace map," which contains detailed information and fully describes the status of each element—the basic information database of cyberspace assets. For important large-scale networks, it is essential to improve the security management of network software and hardware assets. The implementation of cyber defense requires deploying a system for cyberspace asset detection, mastering the network architecture, important nodes, key equipment, and key protection objects, as well as discovering "risk assets." Largely, network offense and defense are represented by the game of exploiting and repairing vulnerabilities in a time window. Using existing databases of cyberspace assets, the network devices and addresses affected by vulnerabilities can be quickly searched in the database as soon as new vulnerabilities are discovered to provide accurate target orientation for active defensive actions and timely fix vulnerabilities.

Strategic early warnings in cyberspace are essential for cyberspace defense strategies. Mastering the behavioral characteristics of cyberthreats and building a platform for threat intelligence support can provide reliable intelligence protection for the implementation of security early warnings. At present, there are hundreds of thousands of hackers in the world. For national-level hacker groups, the defender must always be aware of the technical means, behavioral characteristics, and threatened systems of their attacks, master their attack codes and monitor developmental changes, and assess the potential hazards faced by the existing network to implement effective responses. Even for cyberattacks that occur in other places, mastering their attack codes and behavioral characteristics is crucial for monitoring and warning about threats to our network and mastering cyberspace defense strategies.

Strategic early warnings in cyberspace are essential to comprehensively control security in cyberspace. The traditional single intrusion detection system is outdated, and single-machine antivirus software is prone to failure. It is important to build a complete system supported by big data and cloud technology, focusing on fusion of multisource data and information sharing, and comprehensively integrating various systems. Such a complete system should cover the entire domain and be connected from top to bottom. Thus, the resulting system would have an integrated, distributed structure for a comprehensive safety monitoring and early warning system. This would help us improve our ability to learn about abnormal behaviors, discover potential unknown threats, pinpoint the source of the attack, and anticipate the evolution trend of security incidents.

3 Basic requirements and application styles of strategic early warnings in cyberspace

3.1 Basic requirements for strategic early warnings in cyberspace

A strategic early-warning system in cyberspace should have the ability to discover, track, and identify threats to cyberspace strategies, as well as the traceability capabilities for analysis and decision-making on countermeasures [8]. Thus, such a system needs to have the following basic capabilities:

(1) Comprehensiveness: when it is difficult to judge the severity of the threat, the system should follow the principle of “no misrepresentation” to warn against behaviors that endanger cybersecurity.

(2) Preliminary control: early warnings in cyberspace should be timely, and thus, it is necessary to act depending on the thresholds, analyze and predict a cybersecurity or strategic crisis, and perform early control actions.

(3) Diagnosis: when a network system is built and managed, it is necessary to properly test and diagnose possible network security problems and to record network software and hardware and their status. Based on this, we can analyze and judge the potential harm of various network attack methods.

(4) Dynamic quality: we should closely track the development of new network technologies, the discovery of new problems, and the new changes in environmental factors. These actions are required to timely adjust China’s networks, respond to changes in global cyberattacks, and continuously strengthen the update of analysis and judgment models and countermeasures.

(5) Normative quality: it is necessary to use systematic planning strategies and rational analysis methods to perform procedural decision-making on strategic judgments, countermeasures, and methods for cyber-hazards.

3.2 Application style of strategic early warnings in cyberspace

3.2.1 Early warnings about security vulnerabilities

A vulnerability warning is an early-stage strategic warning. These warnings can be generated by active mining and analysis of security vulnerabilities in important network equipment, operating systems, application software, and application service systems (e.g., domain name system, email system) to discover backdoors, design flaws, and equipment and system management vulnerabilities in the system on time. In this way, the risk can be mitigated as soon as possible to prevent malicious use. These early warnings are mainly provided for security vulnerabilities that have not yet been announced internationally.

3.2.2 Early warnings about security threats

A security threat warning is a medium-term warning. These warnings are based on the deployment of systems for cyberspace asset detection and threat intelligence perception. Such systems discover “risk assets,” track and monitor network security incidents (e.g., the construction of global botnets, the spread of worms, hacking activities, disclosed security vulnerabilities, and the latest methods of network attacks) in real time. Finally, these systems can predict the scope, degree of harm, and duration of potential cyber-destructive attacks on the network security. Thus, we can notify about relevant threats in a timely manner according to regulations and procedures and take countermeasures as soon as possible. These warnings are mainly aimed at threat sources that have appeared elsewhere but have not yet been involved with the protected network.

3.2.3 Early warnings about intrusion attacks

Early warning about intrusion attacks is an imminent warning. These warnings are based on the deployment of systems for network intrusion detection and behavior audit at key locations (e.g., network channel entrances and exits, important servers, and important application systems). These systems monitor network attackers’ penetration of the network, access to important data, and other abnormal behaviors in real time. For the discovered attacks that have been in contact with the protected network, the system raises an alarm and responds in real time. It automatically eliminates the threat using other protection systems. Alternatively, the threat is quickly handled by safety protection personnel. Therefore, such systems prevent large-scale invasion and sabotage, preventing the situation from expanding further.

3.2.4 Early warnings about abnormal behaviors

Abnormal behavior warning is an internal warning that mainly warns of abnormal behaviors or attack attempts that occur in the internal network. The system monitors and audits user operations and network behaviors of important internal networks to promptly discover abnormal situations that directly endanger network security, such

DOI 10.15302/J-SSCAE-2021.02.001

as illegal operations, deliberate sabotage, and virus transmission. The system should track and locate the source of threats accurately.

4 Development status of the strategic early-warning and monitoring system for cyberspace

4.1 Construction of early-warning and monitoring systems for cyberspace in foreign countries

Countries and regions with well-developed information infrastructure focus on the development of strategic early warnings for cybersecurity. Taking the United States as an example, the representative approach is as follows [4].

The first priority is building global network communication data-monitoring capabilities. On one hand, the United States relies on its dominant position as a global information hub to collect basic data on a large scale at important data exchange nodes. On the other hand, it has adopted methods such as transforming and monitoring submarine optical cables to cover the network monitoring range to overseas areas. More than 50% of the traffic in the Internet backbone network is included in the monitoring scope.

Relevant government departments increasingly use the monitoring data from large network operators and Internet service providers. Intelligence agencies identify potential threats by conducting big data correlation analysis on corresponding traffic data, network behavior data, etc. Top backbone network operators such as Sprint, Telephone and Telegraph, Verizon, and Internet service providers such as Microsoft, Google, Facebook, and Apple are all partners of intelligence agencies.

In-depth information cooperation and data sharing have been extensively implemented. The Ministry of Homeland Security, the Ministry of National Defense, and the Ministry of Justice emphasize the interconnection and interoperability of their intelligence and information. They establish a “if one knows, everyone knows” notification system for actions and early-warning intelligence, aiming to link early warnings and responses for system-wide network security. Moreover, the United States has established basic Internet data-sharing mechanisms with the United Kingdom, France, and Germany.

Systems for early warnings and monitoring in cyberspace, such as the “Einstein Plan” intrusion prevention project, aim to support government agencies in responding to cybersecurity threats. Specifically, these systems aim to provide capabilities such as intrusion detection, intrusion prevention, forensic analysis, and information sharing. The “Einstein Plan” is planned and deployed uniformly by the state to monitor the network entrance and exit traffic of various government departments. Once a cyberattack occurs, the monitoring system automatically reports to the United States Computer Emergency Response Team (US-CERT) under the Department of Homeland Security. Security experts review cross-agency security incidents in real time and respond to the emergency [9,10].

4.2 Construction of cyberspace early-warning and monitoring system in China

4.2.1 Laws and regulations level

In terms of cyberspace monitoring, early warnings, and emergency response, the *Cybersecurity Law of the People’s Republic of China* clarifies the responsibilities of functional departments of relevant national and provincial governments. Moreover, the law provides legal protection for national cybersecurity early warnings and security incident handling. The law emphasizes that national cybersecurity and information departments should focus on overall coordination to strengthen the collection, analysis, and notification of cybersecurity information. Information on cybersecurity monitoring and early warnings should be released in a unified manner in accordance with regulations. Relevant departments should establish and improve cybersecurity risk assessment and emergency response mechanisms, and formulate emergency plans for cybersecurity incidents and regular drills. The department responsible for the security protection of critical information infrastructure should establish and improve cybersecurity monitoring, early warnings, and information reporting systems in this field. It should submit information on cybersecurity monitoring and early warnings according to regulations and formulate an emergency response to cybersecurity incidents, as well as plan and organize drills on a regular basis. When the risk of cybersecurity incidents increases, the relevant departments of the government at or above the provincial level should take measures according to specified procedures, characteristics of cybersecurity risk, and possible harm.

4.2.2 Technical level

Many cybersecurity companies have established relatively mature platforms for cyber threat perception analysis, which mainly adopt two methods: (1) Internet online detection and monitoring and (2) important network hub detection and monitoring. The companies extensively collect data on Internet equipment, entrance and exit traffic, and security system operations. Subsequently, big data and artificial intelligence analysis is applied. Thus, the threats to cyber infrastructure and key business networks are detected. To a certain extent, this approach allows to detect cyberattacks early, backtrack intrusion paths, and locate attack sources. Some domestic and foreign cybersecurity companies have established specialized cyberspace surveying and mapping platforms, vulnerability collection and analysis platforms, and opened Internet services that provide data support for strategic early warnings and rapid security incident handling in cyberspace.

4.2.3 Remaining challenges

The following main challenges remain: (1) We do not have a sufficient understanding or a comprehensive database of network assets. Government departments and enterprises in important industries have insufficient knowledge of their own cyberspace assets and lack data that would support situation analysis and emergency response processing. (2) Security monitoring data cannot be shared. Thus, national gateway data, urban area data, and industry intranet data cannot be aggregated. There is a lack of data-sharing mechanisms among units to exchange data on monitoring and threat intelligence. Hence, a comprehensive correlation analysis of cyberattacks cannot be carried out. (3) It is difficult to obtain evidence of cyberattacks. Some units refuse to provide forensic data or delete logs without authorization. This affects the traceability and tracking of cyberattacks and reduces the security of national cyberspace.

5 Key components of a strategic early-warning system for cyberspace

5.1 Cyberspace surveying and mapping system

Cyberspace surveying and mapping systems are the basis for a strategic early-warning system. We can control the situation and initialize defense operations only after fully understanding the software and hardware assets of one’s own cyberspace. To perform cyberspace surveying and mapping, it is necessary to perform large-scale cyberspace software and hardware asset detection as a preliminary task. Supporting technologies include active perception, big data mining and analysis, knowledge learning reasoning, and visual display. This system should strengthen the construction of a cyberspace software and hardware asset base library and in-depth data mining and analysis. The system also needs to realize the multilevel visual display of cyberspace maps.

5.2 Vulnerability collection and early-warning platform

A platform for collecting vulnerabilities and early warnings is the main component of an early-warning system in the initial phase. Vulnerability information can be obtained by independent mining; other sources include vulnerability databases disclosed by relevant institutions in China and abroad and the submissions by individuals. As of March 5, 2021, the global public vulnerability disclosure platform, Common Vulnerabilities and Exposures, contains approximately 1.49×10^5 public vulnerabilities [11], and the China National Vulnerability Database of Information Security contains approximately 1.59×10^5 public vulnerabilities [12]. These vulnerability databases provide basic information, such as the vulnerability name, number, type, source, threat type, hazard level, repair patch, specific equipment affected by the vulnerability, and software version. However, diversified vulnerability information sources have problems, such as inconsistent and unstructured data formats. Professionals are required to perform further data fusion and analysis, verification, and sorting, and unify data structure. The aim is to build a vulnerability warning information database compatible with different data formats, and release and push information directionally on demand. In addition, it is also necessary to pay attention to the adaptability design of the key fields in the vulnerability information database and the software and hardware asset database to provide data support to improve awareness of cyberspace situations and provide rapid threat warnings.

5.3 Threat intelligence perception and push system

The threat intelligence perception push system is the main component of the middle-term warning of the early-warning system, which is divided into two parts: (1) the threat intelligence perception information database and (2) the threat intelligence analysis and push system. The database mainly obtains information by manual collection, automatic sampling, network platform acquisition, and public database queries. The information is analyzed and sorted in the database. Related content includes the addresses that have initiated cyberattacks, devices and domain names used by hackers, malicious code samples such as various viruses and Trojan horses,

DOI 10.15302/J-SSCAE-2021.02.001

vulnerability security threats, hacking behavior characteristics and methods, dangerous hyperlink addresses, malicious software blacklists, and equipment and systems that may be threatened by certain attacks. The threat intelligence analysis and push system mainly targets specific threats, specific protection targets, and newly released vulnerabilities. Using intelligent data mining and matching algorithms, it discovers potential security threats to important targets. The system pushes the intelligence information relevant for early warnings intelligently, automatically, and quickly.

5.4 Safety monitoring comprehensive early-warning system

The comprehensive early-warning system for security monitoring is the main approach for imminent warnings. Such a system is divided into (1) the traffic monitoring and analysis systems and (2) network intrusion forensic and behavior audit systems. The traffic monitoring and analysis system is deployed at the network trunk node and the entrance and exit of each access network. The main purpose of the system is to perform trunk data collection, abnormal network traffic analysis and detection, attack code detection and capture, security event fusion analysis, comprehensive security situation display, staged network data storage return visits, and other functions. Network intrusion forensic and behavior audit systems are deployed in important network systems and key service nodes, mainly for the rapid and accurate positioning of cyberattacks.

6 Countermeasures and suggestions

6.1 Strengthening top-level design and overall coordination

Cybersecurity is related to the overall situation of national security; it is necessary to complete high-quality work on top-level design and coordination of multiple departments. Strategic early warnings, as the primary link and normalization of cybersecurity, should be coordinated in its entirety and conducted based on division of labor. It is recommended that the relevant national competent departments be led by a centralized and unified leadership to coordinate the planning of strategic early warnings in cyberspace. Furthermore, they should coordinate system construction, security risk assessment, and emergency response to major incidents. Based on the division of responsibilities, government departments at all levels and related industries should perform early-warning monitoring and emergency response work collaboratively, according to their respective advantages.

6.2 Focusing on multisource data fusion and intelligence sharing to lay a solid foundation for national cyberspace strategic early warning

Establishing and improving an early-warning and monitoring system for national-level security defense requires the comprehensive collection of Internet access data from government departments, information systems related to the national economy and people’s livelihood, and threat intelligence data from important units. Based on distributed front-end data collection and centralized back-end data analysis mode, the data from multiple sources should be correlated and analyzed. The aggregated and processed intelligence information should be distributed in a timely manner to improve the country’s ability to learn potential abnormal behaviors on the network, detect cyberattacks, and coordinate defense capabilities. The system should issue security warnings fast, take corresponding countermeasures, trace the source when necessary, locate the attacker, and provide support for effectively responding to cyberattacks.

6.3 Strengthening the participation of multiple professional forces and improving the system for strategic early warning in cyberspace

China has established a relatively smooth communication mechanism in terms of security vulnerabilities, Trojan viruses, hacker attacks, etc., and has a robust early-warning system of cybersecurity threats and rapid handling of security incidents [13]. It is recommended to further improve this early-warning system at three levels: national, industry, and unit. The overall coordination of relevant national departments should be used to actively guide the participation of capable units such as universities and research institutes. They can analyze vulnerabilities of operating system software and important information system software and hardware products, and timely discover and eliminate various preset backdoors and design flaws. The professional force for cybersecurity protection in the network application industry is responsible for the analysis and detection of vulnerabilities of special software and important application software in this industry, and finding security vulnerabilities in the process of information system development and integration. They should also formulate quantitative assessment and inspection standards, and conduct regular security risk assessments and inspections of the internal networks of the industry. The cybersecurity protection forces at the unit level should conduct security risk assessment and inspection of the internal networks of the corresponding and lower-level units, find security vulnerabilities, and suggest improvements for the network information systems within the scope of their protection.

6.4 Performing regular safety assessments for early diagnosis and early detection of hidden dangers

Cybersecurity is a relatively new and dynamic field. It is necessary to constantly search for and discover problems in network applications and mitigate risks in advance. This is the most important aspect for implementing an early-warning system for cybersecurity. Regular security assessments should be strengthened within the industry, and relevant government departments should organize cybersecurity assurance drills to identify hidden dangers in a timely manner and implement countermeasures as soon as possible. This approach helps rapidly and continuously improve cybersecurity protection capabilities.

6.5 Implementing a threat grading mechanism for early warnings; standardizing and refining supporting response measures

Early warnings about terrorist threats in the United States, Russia, and other countries are generally divided into three levels. For example, the United States use warning announcements, escalation warnings, and emergency warnings. Russia uses three colors, blue, yellow, and red, which classify levels of threats from low to high [14]. China’s strategic early warnings in cyberspace can rely on existing practices of handling international terrorist threats. We can classify threats as blue, yellow, and red and propose different countermeasures for different levels. Blue early warnings indicate the discovery of major vulnerabilities and major cyberattacks, occurring overseas, which may harm China’s cybersecurity. Yellow code is intended for situations when the spread of harmful viruses and worms or large-scale cyberattacks may cause major harm; such attacks aim at China and are performed by hacker organizations. Red code indicates large-scale disruptive and paralyzed attacks by hostile forces and terrorist organizations on China’s network infrastructure and important information systems related to the national economy and people’s livelihood, when the expected consequences are particularly serious.

6.6 Using the advantages of Internet companies to build a strategic early-warning team for cyberspace

Enhancing the sense of mission and responsibility of Internet companies in the field of cybersecurity, jointly promoting the sustainable development of the Internet industry, and ensuring the steady growth of enterprises is not only the goal of enterprises but also the need of national development. Cybersecurity strategy for early warnings should use the advantages of Internet companies in cyberspace surveying and mapping, vulnerability mining, cybersecurity monitoring, big data analysis, etc., in terms of technology, products, data, and talent. The cybersecurity strategy should guarantee the creation of a team that would cover important networks related to the national economy and people’s livelihoods. This team can comprehensively respond to various major threats in cyberspace and quickly address major security incidents.

References

[1] Zhang F, Qin Z G, Liu J D. Intrusion event based early warning method for network security [J]. Computer Science, 2004, 31(11): 77–79, 129. Chinese.

[2] Chen M, Wang Q B, Tang W Q. The capability of strategic intelligence supporting for cyberspace security [J]. Journal of Intelligence, 2020, 39(4): 127–131. Chinese.

[3] Gong J, Zang X D, Su Q, et al. Survey of network security situation awareness [J]. Journal of Software, 2017, 28(4): 1010–1026. Chinese.

[4] Wu T. Situation and challenges of overseas information network monitoring [J]. National Defense Technology, 2016, 37(3): 40–43. Chinese.

[5] Li H F, Tian K S, Jin H B. Analysis on strategic early warning aerospace target and identification [J]. Aerodynamic Missile Journal, 2015 (6): 30–33. Chinese.

[6] Xuan L, Su J S, Miao Q, et al. Study on network security strategic indication/warning system [J]. Communications Technology, 2001 (7): 90–92. Chinese.

[7] Liu F Z, Xiao B, Liu J, et al. Analysis on the development of American strategic early warning system [J]. Aerodynamic

DOI 10.15302/J-SSCAE-2021.02.001

Missile Journal, 2019 (3): 65–69. Chinese.

[8] Feng W, Mei Y. In the era of big data, data sovereignty rises and falls [J]. Information Security and Communications Privacy, 2015 (6): 49–51. Chinese.

[9] Yu F. “Einstein plan” upgrades American cyber security [J]. Confidential Work, 2013 (8): 54–55. Chinese.

[10] Zhao Y G, Huang H B. American “Einstein plan” research [J]. Journal of Information Security Research, 2020, 6(11): 1013– 1016. Chinese.

[11] Common Vulnerabilities & Exposures Numbering Authorities. Common vulnerabilities and exposures [EB/OL]. (2021-03-05) [2021-03-06]. http://cve.mitre.org/cve/.

[12] China National Vulnerability Database of Information Security. Vulnerability information [EB/OL]. (2021-03-05) [2021-03-06]. http://www.cnnvd.org.cn/web/vulnerability/querylist.tag. Chinese.

[13] Zhou Y L. Computer network emergency response and internet emergency coordination system in China [J]. World Telecommunications, 2004 (3): 33–38. Chinese.

[14] Dai Y M. Research on Russian anti-terrorism mechanism [J]. Russian, Central Asian & East European Studies, 2012 (5): 31–38, 95–96. Chinese.