AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Technology and Applied Sciences
ISSN (E): 2832-1766 Volume 29, October - 2024

US AND CHINA EXPERIENCE IN ENSURING CYBERSECURITY AND THEIR FEATURES

Sobirov Anvar
Scientific Researcher
E-mail: dilm79@inbox.ru Mobile +998997700429

ABSTRACT

The essence of cybersecurity as a social phenomenon is the state and quality of the actual social relations in society that provide the necessary level of guarantees for its security, and allow the state to predict, promptly identify, prevent and eliminate real and potential dangers and threats to national interests.

KEYWORDS

National cyber strategy, cyber command, training of specialists in the field of cybersecurity, and enemy cyberspace.

Introduction

The essence of cybersecurity is manifested, firstly, in the availability, constant increase and enrichment of various resources and capabilities of society, their rational use for the implementation of national interests, sustainable and progressive development of the country, secondly, in the functioning of an effective system of counteracting dangers and threats to national interests, adequate to their scale and level, and, thirdly, in the dynamism of the national security system and its ability to promptly identify and neutralize dangers and threats to national interests, promptly restructure in accordance with changing circumstances.

The USA

The United States historically became one of the first countries to consider cybersecurity as a matter of strategic importance. The main provisions of the US cybersecurity strategy were formed in the 1990s. "In 1995, the Clinton Administration released the National Security Strategy, which outlined the task of achieving information superiority through offensive and defensive information operations" (Clinton William. National Security Strategy. 2015)

Presidential Directive No. 63 "On the Protection of Critical Infrastructure" was further developed in the form of codification in the "National Cyberspace Security Strategy" and in the Homeland Security Presidential Directive No. 7 "On the Identification, Prioritization, and Protection of Critical Infrastructure Elements" (Homeland Security Presidential Directive. 2003). These documents define the basic principles and tasks of ensuring cybersecurity: preventing cyberattacks against critical infrastructures; eliminating vulnerabilities in critical infrastructures; and minimizing potential damage in the event of a successful cyberattack. The possibility of the use of cyber weapons by the United States as a defensive measure is also outlined. In 2008, the "Comprehensive National Cybersecurity

Initiative" was created. This initiative assumed the solution of a number of tasks to ensure the cybersecurity of the United States" (The National Strategy to Secure Cyber Space. 2003)

1. Protecting national databases from attacks by potential adversaries.
2. Ensuring that federal government specialists are aware of the existence of vulnerabilities and security threats in national computer networks and critical infrastructures.
3. Expanding the technical and operational capabilities of US counterintelligence agencies.
4. Creating a system for training specialists in the field of cybersecurity.

In 2017, the US Cyber Command unit was transformed into a unit of the Strategic Command" (News.com, 1999-2020). "The Pentagon has given the US Cyber Command the ability to take a tougher approach to not only protecting against hacker attacks but also intrusions into the cyberspace of other states. The agency has been given the authority to carry out preventive cyberattacks on the digital infrastructure of adversaries. At the same time, actions to protect the United States from cyberattacks should primarily take place in the enemy's cyberspace. An example of the implementation of a preventive approach to ensuring cybersecurity is the US Cyber Command's initiative to introduce malware into the enemy's cyberspace" (U.S. Cyber Command's Malware…2019).

In September 2018, President Donald Trump signed the US National Cyber Strategy. At the same time, the 2018 document largely repeats previous US documents in the field of cybersecurity.

"The National Cyber Strategy identifies active adversaries of the United States operating in cyberspace. In particular, it is noted that Russia, Iran, North Korea, and China carry out cyberattacks that damage the American and international economies, as well as commit acts of economic espionage against the United States and its allies" (Cyber Strategy 2018).

The National Cyber Security Strategy consists of 4 parts, each of which corresponds to a specific direction of US policy:

1) Protect the American People, the Homeland, and the American Way of Life;
2) Promote American Prosperity;
3) Preserve Peace through Strength;
4) Advance American Influence.

The first part, "Protect the American People, the Homeland, and the American Way of Life," sets out the goal of ensuring proper risk management in the field of cybersecurity, increasing the safety and security of information systems and information of national importance. The goal of the first part is achieved by protecting federal networks and information, protecting critical infrastructure, combating cybercrime, and improving incident reporting, including giving the Department of Homeland Security broader authority to oversee civilian cybersecurity efforts and cooperating with other countries to combat cybercrime. The threats to U.S. cybersecurity listed in the document can be structured as follows:

1) Disruption of federal department and agency networks;
2) Poor quality of IT products and services in the U.S. federal supply chain;
3) Unreliability of federal contractors with access to state secrets;
4) Use of outdated IT products or standards by government agencies;
5) Destabilization of critical infrastructure;
6) Cyberattacks on election infrastructure, transportation, maritime, and space infrastructure.

The second part of the US national cybersecurity strategy - "Promote American Prosperity" aims to maintain the influence of the United States in the technology ecosystem and develop cyberspace as an engine of economic growth, innovation and efficiency.

The implementation of the goal of the second part of the strategy involves: developing a viable and efficient digital economy; encouraging and protecting US ingenuity; creating a qualified personnel reserve; collaborating with IT companies to test cybersecurity in new products; and attracting and retaining highly qualified cybersecurity personnel. At the same time, the second part of the cyber strategy presents a number of measures to ensure US cybersecurity and international security, including:

1) Creating uniform international cybersecurity standards;
2) Creating cybersecurity standards for the next-generation digital infrastructure;
3) Economic and political support for American-made IT products in the field of cybersecurity;
4) Strengthening counterintelligence measures in the field of IT technologies;
5) Financing school and university IT education programs;

Part III, "Preserve Peace through Strength," sets out the goal of "identifying, countering, disrupting, deterring, and deterring cyber activities that are destabilizing and contrary to national interests while maintaining U.S. superiority in and through cyberspace." This goal is to be achieved by establishing norms of responsible state behaviour and deterring inappropriate behaviour in cyberspace. The strategy states that the administration will use "all instruments of national power" to prevent cyberattacks and take swift and effective action against adversaries. Part IV, "Advance American Influence," aims to preserve the long-term openness, interoperability, security, and reliability of the Internet that is supported and strengthened by U.S. interests.

The goals of Part IV include: promoting an open, international, reliable, and secure Internet; building international cyber capabilities; and jointly countering threats to mutual interests. Thus, the US policy in the field of cyberspace and cybersecurity is primarily aimed at achieving information superiority. Along with the tasks of ensuring cyberspace security, the regulatory documents reviewed outline political goals and list the main opponents of the US in cyberspace - Russia, China, Iran, the DPRK and international terrorist organizations. It is indicated that the listed actors use cyberspace for military and political purposes, and regularly conduct cyberattacks against the US and its allies, without providing any significant evidence.

China

PRC. In 2000, an attempt was made in China to classify potential offences in the information sphere, which resulted in the "Resolution of the National People's Congress on the Protection of the Internet Space", which identified areas in which violations were possible: economic, educational, maintaining social stability and protecting citizens" (Razumov. 2017). In 2002, China's defence policy was formed and published, which placed "emphasis on the modernization of the armed forces of the PRC, in particular their informatization" (National Defense of China. 2002). In 2003, the Resolution of the State Leading Group for Work in the Field of Strengthening Information Security was published. The document assigns to responsible persons the need to "take steps to strengthen the protection of strategic infrastructure, monitor the Internet space for possible threats to the PRC, and develop measures to attract qualified specialists in the field of information security. Since 2004, the PRC has been

implementing the state program "Golden Shield", the essence of which is to filter Internet traffic between Chinese cyberspace and the rest of the world. In fact, the program "Golden Shield" is an attempt by the Chinese government to exercise total control over cyberspace in order to limit Chinese citizens' access to foreign Internet resources, mass media and social networks" (Ventre. 2024).

In 2006, the "State Strategy for the Development of Informatization for the Period from 2006 to 2020" was adopted. "This document emphasizes the high importance of control over information technology. It is proposed to create special structures to regulate processes in the information environment. It is envisaged to establish a vector for the development of information technology and state policy in this area. The strategy includes the creation of its own software, as well as a combination of military and civilian products" (Razumov. 2019)

The idea of sovereign cybersecurity was further developed in the provisions of the new National Security Law adopted in China in 2015, which emphasized the need to strengthen the protection of national information systems and establish cyberspace sovereignty in China. "These issues are discussed in more detail in the cybersecurity law, which provides for mandatory registration in Internet services under real names, the involvement of private operators in government investigations, the introduction of many obligations to store personal data in China, which must be stored only in the country. In 2016, the law was finally adopted, and in 2017 it came into force" (Yan. 2018).

"Part of the content of the law repeats existing rules adopted by China over many years and simply combines individual regulations into one. Previously existing rules were scattered across different regulations. The Chinese government, when adopting this law, was largely guided by the position that the formation of a unified law improves the effectiveness of legal regulation of cyberspace, and to a greater extent informs the business community, as well as the general public, about the unprecedented threats to cybersecurity within and beyond the borders of China" (Lindsay. 2015).

The law defines a number of terms related to cybersecurity. According to Article 76, cybersecurity refers to the adoption of necessary measures to prevent cyberattacks, “intrusions, interference, destruction and illegal use, in order to ensure stable, reliable operation and confidential functioning of the network. Networks are considered here as systems consisting of computers and other information devices or objects used for “collecting, storing, transmitting, exchanging and processing information. Personal information refers to all types of information, recorded electronically or by other means, taken alone or together with other information, sufficient to identify an individual, including natural persons: full names, dates of birth, national identification numbers, personal biometric information, addresses, telephone numbers.” (Rogozhin. 2020). Article 31 of the Cybersecurity Law of the People's Republic of China states that "the state shall focus on protecting critical information infrastructure in the fields of public relations, information services, energy, transportation, water conservancy, finance, public services, e-government and other key elements of the information infrastructure, the disruption of which will cause damage to national security, the national economy and endanger the lives of citizens. Critical information infrastructure operators must store key data and personal information within the territory of the People's Republic of China. In cases where "it is necessary to provide information to external agents, the security assessment shall be carried out in accordance with the measures formulated by the national cyberspace administration authority jointly with the relevant departments of the State Council. Network operators shall have legal obligations under this law."

Conclusion

The law also establishes the fundamental principle of promoting and protecting national sovereignty in cyberspace within the framework of networks. The list of additional obligations for network operators includes:

1. compliance with the requirements of a multi-layered cybersecurity protection system;
2. authentication of the real identity of users;
3. development of strategies for emergency response in the field of cybersecurity;
4. Provide assistance and support to investigative bodies.

Also, "the law regulates the activities of Internet media and social networks. All content produced on the network is stored on the territory of the PRC for 6 months. The law pays special attention to the identification system: in order to carry out any activity on the network, Chinese citizens must confirm their identity and undergo the appropriate verification procedure, in other words, the law prohibits Internet anonymity.

Thus, the Cybersecurity Law, on the one hand, protects critical information infrastructure facilities of the PRC from cyber threats associated with the theft of personal data and warns against cyber espionage, and on the other hand, provides special services for the PRC with the opportunity for physical access to data of critical information infrastructure facilities. Despite the fact that the law uses the concept of "cybersecurity threat", cyber threats are mainly considered within the framework of critical information infrastructure and information networks and are presented by rather general definitions, such as theft of personal data, disruption of functioning, etc.

References

1. China. - 2002. - Access mode: http://www.scio.gov.cn/zfbps/ndhf/2002/Document/307925/307925.htm (date accessed: 11.05.2020).
2. Clinton William. National Security Strategy / Washington DC: Government Printing Office. February 1995. P. 8.
3. Cyber Strategy 2018 [Electronic resource] / Department of Defense Summary – 2018 - Access mode: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (date of access: 10/01/2018).
4. Lindsay J. R. The Impact of China on Cybersecurity / J.R. Lindsay // International Security. - 2015. - vol. 39. - p. 153. - Access mode: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2849&context=lawreview
5. Razumov E.A. China's cybersecurity policy [Electronic resource] / E.A. Razumov // Russia and the Asia-Pacific region. 2017. No. 4 (98). P. 158 Access mode: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti (date of access: 11.05.2020).
6. Rogozhin A.A. PRC - Cybersecurity Law Adopted [Electronic resource] / A.A. Rogozhin - Access mode: https://www.imemo.ru/news/events/text/knr-zakon-o-kiberbezopasnosti-prinyat. (date accessed: 04/20/2020).

7. The Comprehensive National Cybersecurity Initiative [Electronic resource] // The White House. - 2008- Available at: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurityinitiative (Accessed on 05/15/2020).
8. The National Strategy to Secure Cyber Space / The White House, Washington DC, USA, 2003 // The White House. 2003. Access mode: http://georgewbush-whitehouse.archives.gov/pcipb/ (date of access: 02/25/2018). Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. // U.S. Department of Homeland Security. 12/17/2003. Available at: https://www.dhs.gov/homeland-security-presidential-directive-7 (Accessed on 02/25/2020).
9. The Pentagon Changed the Strategy of the US Cyber Command [Electronic resource] // News.com, 1999-2020. - Available at https://www.newsru.com/world/18jun2018/cyber.html. (Accessed on 03/23/2020).
10. U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace [Electronic resource] // Council of Foreign Relations. – Access mode https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace. (date of access: 03/23/2020).
11. Ventre D. Chinese Cybersecurity and Defense. London / D. Ventre // WileyISTE Publ., - 2014. - 301 p.
12. Yan S. China's new cybersecurity law takes effect today, and many are confused / S. Yan // CNBC. - 2017. - Access mode: https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html (accessed: 13.03.2018).