European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.06.03.47

AMURCON 2020
International Scientific Conference

ENSURING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE IN RUSSIA AND CHINA

Ella Gorian (a)*, Kristina Horian (b)
*Corresponding author

(a) Vladivostok State University of Economics and Service, 41 Gogolya St., Vladivostok, Russia, ella.gorian@gmail.com
(b) Vladivostok State University of Economics and Service, 41 Gogolya St., Vladivostok, Russia, kristina.gorian@gmail.com

Abstract

The security of critical information infrastructure is a core issue of a national cybersecurity mechanism. Each state develops a specific regulatory and institutional mechanism of regulation. Russia and China both pursue the digital nationalism model. The advantages and disadvantages of the Russian and Chinese national mechanisms are determined. The need and possibility of implementation of the Chinese positive practice is considered. A few general scientific (system-structural, formal-logical and hermeneutic methods) and special legal methods of cognition (comparative legal and formal-legal methods) are being used. The Chinese mechanism for ensuring the security of critical information infrastructure is undergoing the formation phase. The specific Russian federal act clearly defines the CII sectors and the system of state authorities with the strict distribution of their powers. The Chinese mechanism envisage the extension of the CII sectors by executive regulations. The structure of institutional mechanism is undefined and there is a partial duplication of the powers of some authorities. The formation of the Chinese mechanism is complicated by the need to simultaneously achieve goals in the spheres of national security and economy (in the aspect of opposing the US economic expansion into the Chinese market). Both the Russian and the Chinese mechanisms reflect the features of national security systems of each state. The positive practice of People's Republic of China is to be considered in the aspect of simultaneous achievement of national security and economic goals.

Keywords: Cybersecurity, critical information infrastructure, digital nationalism

https://doi.org/10.15405/epsbs.2021.06.03.47
Corresponding Author: Ella Gorian
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Last few years states have been taking active steps to improve national information security mechanisms: the most vulnerable and critical for the functioning of society and the state information infrastructure objects are being determined, the authorized entities are being established, their powers are being distributed, rules and principles of interaction for all participants in information sphere are being established, etc. (Whyte, 2020). Cybersecurity issues are important not only from the standpoint of ensuring the national security of a particular state, but also in other seemingly unrelated areas: the "trade war" that has been lasting for many years between the US and China affects not only the issues of trade tariffs and barriers. The confrontation between the world's first economies concerns, first of all, a market access in key technology sectors and lowering barriers to cross-border trade - it is the digital economy that is on the agenda of many years of negotiations, which the Chinese officials try to exclude from the negotiation process. But the United States insist on the continuity of the trade dispute settlement with the harmonization of regulations in the field of information security and personal data protection, as well as cloud technologies (Wei, 2019).

The Cybersecurity Law of the People's Republic of China of 2017 has established general principles and directions for the development of national regulation in the field of information security of the state, however, the special rules relating to certain issues (critical information infrastructure (CII), personal data) are under development and approval. The Chinese legislator is faced with the difficult task of building a balanced regulatory mechanism for ensuring the security of the CII, since it is necessary to take into account the interests of national security and maintain the attractiveness of the Chinese market for investment.

The formation of the Russian national cybersecurity mechanism is on the stage of implementing the provisions of federal law on the "autonomous Internet" (Horian & Gorian, 2020). As it was noted before (Gorian, 2020), Russia, like China, implements the so-called "digital nationalism" model, which features the enhanced state responsibility for ensuring the security of information and information systems (including CII). This model is embodied in special legal regimes for the data flow and protection, including personal data (Alekseenko, 2019, 2020). So the comparison of Russian and Chinese models is important for studying the positive experience of the latter and for the refining the Russian approach to CII protection.

2. Problem Statement

Critical information infrastructure is the primary target of cyber-attacks. The most high-profile attacks in recent years have been targeted the communication networks of health services, transport, energy, financial and banking systems. These sectors are of critical value for the life and well-being of society and the state. Therefore, such attacks can be countered by creating a robust national mechanism: state develops a regulatory framework and delegate powers to special cybersecurity authorities, emergency departments or other national regulatory authorities responsible for the implementation of operational tasks (Chaudhary et al., 2018). Harmonization of regulatory and institutional mechanisms is a major challenge for the legislator.

https://doi.org/10.15405/epsbs.2021.06.03.47
Corresponding Author: Ella Gorian
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

3. Research Questions

The completion of a comparative study on the security of critical information infrastructure in Russia and China requires the finding of answers to the certain research questions. First, the relevant legal and regulatory framework is to be analysed. Then, the structure and competence of the state authorities in Russia and China are to be characterised. Finally, the need and possibility of the Chinese practice implementation to be determined.

4. Purpose of the Study

The purpose of the study is to determine the advantages and disadvantages of mechanisms for ensuring the security of critical information infrastructures of the Russian Federation and the People's Republic of China and to formulate proposals for improving the Russian mechanism.

5. Research Methods

In this study we will use the general methods (system structural, formal logical and hermeneutic ones) as well as the special legal methods of scientific knowledge (comparative legal and formal legal methods).

6. Findings

The national legal mechanism of cybersecurity comprises two sub mechanisms: the regulatory and the institutional ones. First, we have to characterise the Russian and Chinese normative mechanisms.

Russian Federation. Information security in Russia has always been and remains an important part of national security. In 2018, for the first time at the legislative level, the importance of CII for state security was recognized and reflected in a Federal Law of the Russian Federation "On the security of the critical information infrastructure of the Russian Federation" (hereinafter - FZ-187). The criminal legislation was supplemented by a rule establishing liability for unlawful influence on the CII (Article 274.1 of the Criminal Code of the Russian Federation).

FZ-187 defines the concepts of "critical information infrastructure" (Art. 2 (6)), "objects of critical information infrastructure" (Article 7) and "subjects of critical information infrastructure" (Art. 2 (8)). Moreover, the law establishes the criteria for classification of objects as CII: these are of social, political, economic, environmental significance, as well as of significance for "ensuring the country's defence, state security and law and order" (Article 7 (2)). Thus, CII comprises such sectors as health care, science, transport, communications, power, banking and finance, the fuel and energy complex, nuclear energy, defence, rocket and space industry, mining, metallurgical and chemical industries.

As part of the implementation of FZ-187, a number of subsidiary legislative acts have been adopted that regulate the procedure for exercising state control, categorizing CII facilities and countering computer attacks.

People's Republic of China. Since 2014, the issues of defining and protecting CII have been raised in every speech of the head of the PRC at government meetings and national conferences on cybersecurity.

https://doi.org/10.15405/epsbs.2021.06.03.47
Corresponding Author: Ella Gorian
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

In his 2016 speech on cyber strategy, Xi Jinping emphasized the importance of protecting such CII sectors as finance, energy, telecommunications, and transportation, and urged the government to accelerate work on building a national CII security mechanism. The Cybersecurity Law of the PRC was adopted in 2016, and the protection of CII has been linked to building the capacity of the national cyber industry, consolidation and centralization of platforms for collecting information on cybersecurity (Lee, 2018; Lu, 2018).

The law comprises the seven chapters: (1) general provisions; (2) cybersecurity support; (3) network operation security, which includes two sections: general provisions and operation security of CII; (4) network information security; (5) monitoring, early warning and emergency response; (6) legal liability; (7) supplementary provisions.

The legal protection regime is established by Chapter 2 of the Law, and information and communication services, energy, transport, water management, finance, government services and government e-mail services are identified as the CII sectors. State Council of the People's Republic of China is entrusted with the responsibility of regulation of CII identification and the security measures for their protection. The operators of the CII are responsible for the security of the CII objects. All personal data used by CII operators must be stored in China and is the subject to national security checks if it is transferred abroad (Greenleaf & Livingston, 2016). Cyberspace Administration of China has been designated as the body responsible for planning and coordinating measures to protect CII.

It should be noted that a specific feature of the Chinese legal system is the existence of the array of subsidiary legislation acts that supplement and clarify the regulatory requirements of laws. Since the adoption of Cybersecurity Law a number of regulations and orders in the field of CII protection has been developed: the National Cyber Security Inspection Operation Guide 2016, the draft Critical Information Infrastructure Security Protection Regulations, containing an expanded (comparing to the Cybersecurity Law) list of CII sectors (health care, education, social security and environmental protection, research and production (defence industry, mechanical engineering, petrochemical, food and pharmaceutical industries), information (broadcasting and news services), radio and television networks and the Internet, service providers providing cloud computing, big data and other large publicly available information and network services); Cyber Security Review Measures 2020, that imposes the obligation on CII operators to undergo security checks of the network products and services used, which may affect China's national security.

The institutional mechanism of cybersecurity features the state authorities empowered to regulate the use of CII. Following are the characteristics of the Russian and Chinese institutional mechanisms.

Russian Federation. FZ-187 establishes a balanced and coordinated institutional mechanism for ensuring the security of the CII: in addition to the state authorities implementing general measures for the security of the CII (Article 6) there is a special state system for detecting, preventing, and eliminating the consequences of computer attacks on information resources (Article 5). The first includes the President of the Russian Federation, the Government of the Russian Federation, the Federal Service for Technical and Export Control, the Federal Security Service and the Ministry of Digital Development, Communications and Mass Media.

A special role in the support mechanism is played by a special state system for detecting, preventing, and eliminating the consequences of computer attacks on information resources, which performs the

https://doi.org/10.15405/epsbs.2021.06.03.47
Corresponding Author: Ella Gorian
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

functions of protecting the CII. It includes divisions and officials of the Federal Security Service, representatives of CII subjects who take part in the detection, prevention and elimination of the consequences of computer attacks and in responding to computer incidents, as well as the National Coordination Centre for Computer Incidents created by the Federal Security Service, operating on the basis of the corresponding provision.

People's Republic of China. The Cybersecurity Law of the PRC does not contain norms that determine the structure of the institutional mechanism for ensuring the security of the CII, as in the Russian Federation. Analysis of the regulatory framework for ensuring information security allows us to distinguish the bodies of general and special competence, endowed with appropriate powers in the sphere of CII security. The former includes the State Council, the Ministry of Public Security (represented by the Cyber Security Bureau) and the Ministry of Industry and Information Technology. The organs of special competence are the Cyberspace Administration of China and the high-level inter-ministerial control body for cybersecurity, formed by representatives of eleven ministries and departments: the Commission for National Development and Reforms; the Ministry of Industry and Information Technology; the Ministry of Public Security; the Ministry of National Security; the Ministry of Commerce; the Ministry of Finance; the People's Bank of China; the State Administration for Market Regulation; the National Radio and Television Administration; The National Administration of State Secret Protection; the State Cryptography Administration.

However, even within this mechanism, there is a partial duplication of the powers of the Ministry of Public Security as a regulator for management measures for multi-level information protection and the Cyberspace Administration of China as a regulator of critical information infrastructure, which, according to experts, may complicate the process of identifying CII objects and determining CII subjects (Webster et al., 2019).

7. Conclusion

Both regulatory and institutional mechanisms for ensuring the security of critical information infrastructure in Russia and China are determined by a special normative act of the highest nature.

The Russian law directly establishes the list of CII sectors, while the list of CII sectors in the Chinese law is expanded by the inclusion of new sectors by the relevant subsidiary legislation acts, that indicates the growing role of standards adopted by the responsible authorities, in particular, the Cyberspace Administration of China, the Ministry of Industry and Information Technology and the Ministry of Public Security. A similar situation is observed with respect to the authorized state bodies: the Russian law contains such a list with the distribution of powers between them in the field of CII security, while the Chinese law does not contain such rules.

Despite many existing and emerging sources of legal regulation of critical information infrastructure, the regulatory mechanism for ensuring its security is interconnected and reflects the general nature of China's digital policy regime. The Cybersecurity Law establishes the general norms, subsidiary legislation - special rules and standards containing technical and methodological recommendations that can clarify the possible ambiguity of general and special norms. The institutional mechanism is represented by state bodies of general and special competence, however, there is a problem of partial duplication of powers.

The formation of the Chinese mechanism is complicated by the need to simultaneously achieve goals in the spheres of national security and economy (in the aspect of opposing the US economic expansion into the Chinese market). Both the Russian and the Chinese mechanisms reflect the features of national security systems of each state. The positive practice of People's Republic of China is to be considered in the aspect of simultaneous achievement of national security and economic goals.

Acknowledgments

The reported study was funded by RFBR, project number 20-011-00454 "Ensuring the rights of investors in the banking and financial sectors in the context of the digitalization of the economy in the Russian Federation and the leading financial centres of East Asia: a comparative legal aspect".

References

Alekseenko, A. (2019). New Russian model BIT and the practice of investment arbitration. *Manchester Journal of International economic Law, 1*(16), 79-93.

Alekseenko, A. (2020). Russian approach to ICO regulation. *Revista Genero & Direito, 4*(9), 874-881.

Chaudhary, T., Jordan, J., Salomone, M., & Baxter, P. (2018). Patchwork of confusion: the cybersecurity coordination problem. *Journal of Cybersecurity*, *4*(1), 1-13. https://doi.org/10.1093/cybsec/tyy005

Gorian, E. (2020). Genesis of Russian cyber security legal mechanism: an authentic or a trend alike model? In Denis B. Solovev (Ed.), *Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Proceeding of the International Science and Technology Conference "FarEastCon-2019"* (pp. 937-949). Springer.

Greenleaf, G., & Livingston, S. (2016). China's New Cybersecurity Law – Also a Data Privacy Law? *Privacy Laws & Business International Report*, (144), 1-7.

Horian, K., & Gorian, E. (2020). Information security ensuring in the financial sector as part of the implementation of the National Program "Data Economy Russia 2024". *Advances in Economics, Business and Management Research: Proceedings of the International Scientific Conference "Far East Con" (ISCFEC 2020), 128*, 635-644. https://doi.org/10.2991/aebmr.k.200312.091

Lee, J. -A. (2018). *Hacking into China's Cybersecurity Law*. R https://ssrn.com/abstract=3174626

Lu, X. (2018). *Scoping Critical Information Infrastructure in China*. https://thediplomat.com/2018/05/scoping-critical-information-infrastructure-in-china/

Webster, G., Sacks, S., & Triolo, P. (2019). *Three Chinese Digital Economy Policies at Stake in the U.S.–China Talks*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/three-chinese-digital-economy-policies-at-stake-in-the-uschina-talks/

Wei, L. (2019). *U.S. Trade Negotiators Take Aim at China's Cybersecurity Law*. https://www.wsj.com/articles/u-s-trade-negotiators-take-aim-at-chinas-cybersecurity-law-11553867916

Whyte, C. (2020). Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare. *Journal of Cybersecurity*, *6*(1), 1-17. https://doi.org/10.1093/cybsec/tyaa013