Studying the Legal Support of Information Security in the People's Republic of China

Alfiya Rafisovna Alikberova [1], **Svetlana Yur'evna Glushkova** [2], **Eduard Shabanovich Alikberov** [3]

[1]*Kazan Federal University*
E-mail: alfiakasimova@gmail.com

[2]*Kazan Federal University*
E-mail svetaelina@gmail.com

[3]*Kazan Federal University*
E-mail: eduard_alikberov@mail.ru

Abstract

Despite the importance of preserving information, it seems that this right does not have absolute protection. Restrictions and interferences by governments and public authorities in the legal field have been justified in order to create public order and security. The security of the country, the order of the judicial officers to detect crimes and the existence of normal laws such as the anti-money laundering law are among the things that deserve attention in this field, which of course, with the daily need and more than protecting the privacy of people, especially in the field of The challenge of new communication technologies, the involvement of governments and public authorities in the allocation of this type of support, seems acceptable to the extent that it is necessary to protect the rights of citizens, not to conflict with the rights of individuals, and to provide services and proper social management in a precise and defined manner. May it not go to the extent that the freedoms of individuals are sacrificed to the power of governments? The presented work is devoted to such research topics as information conflict and information security. The article presents the results of research on organizational and legal support of information security in the People's Republic of China, as an important subject of international relations at the present stage. The relevance of this research is confirmed by the fact that there is no clear paradigm of information conflict in the domestic and foreign discourse of international relations; at the moment, there is no reliable and sufficiently extensive theoretical base that would allow us to classify, model and study in depth the information conflicts of our time. The study of the People's Republic of China's experience will fill these gaps in scientific and practical terms. The study used general humanitarian research methods: generalization and comparative-historical methods which allowed us to draw reliable conclusions. The presented work would present interest to practitioners of international relations, historians and political scientists, as well as teachers of educational programs related to international relations and information security.

Keywords: Legal support, law, information security, information conflict, People's Republic of China, China, international relations.

Introduction

This work is devoted to the study of a phenomenon called "information conflict", or "information war", "information confrontation". The emergence and existence of this phenomenon have been studied in many disciplines, including history, sociology, conflict studies, psychology and sociopsychology, political science, and, above all, military affairs and international relations. Information conflict, from the point of view of modern science, is a type of conflict between subjects of international relations. The use of its tools and methods is most inherent to international conflicts of the late XX – early XXI centuries. The parties to the information conflict pursue a variety of goals, typical of traditional wars, and completely new, proper only for the modern information society. This article presents the results of research on organizational and legal support of information security in the People's Republic of China as an important subject of international relations at the present stage.

The choice of the People's Republic of China as the object of research is due to the fact that this state experiences a continuous state of information conflict with other subjects of international relations over the past years. Besides, unlike the USA, the UK, France and Germany (which are also considered major players in information conflicts of the time), China holds a largely defensive position in the global information confrontation, because China did not develop overseas propaganda in the second half of the twentieth century, preferring to use means of information influence just inside the country. In the twenty-first century, the PRC is becoming the target of information and psychological attacks aimed at discrediting the political campaigns of their governments. For the PRC, important information conflicts were the unrest in the Xinjiang Uyghur and Tibetan Autonomous regions [1], Hong Kong, and the emergence and fight against the COVID-19 pandemic.

What do you know about intellectual property in cyberspace? Today, many people are active in cyberspace in various ways. These people, who somehow share a part of their career, writing, poetry, etc. with others, have a lot of worries about losing ownership of these contents. Since most of these contents originate from the minds, creativity and ideas of these people, it is a subset of intellectual property in the virtual space, and for anyone who works in this field, it brings such challenges.

Therefore, we have two classifications in the field of intellectual property: industrial property and artistic literary property and related rights. In the field of industrial property, rights and laws help to develop the economy, industry and production of a society; In fact, when an invention is made or a design or an idea is formed, the conditions for supporting it must be provided so that there is no scope for abuse. In the literary and artistic category, we are also facing the field of culture and society, and this part is mostly related to artists, authors, writers, etc. What appears from these works in the virtual space are: books, paintings, photos, articles, etc., which are digitized and republished in the cyber space. The other category is related to the virtual space itself, which includes information, website design, etc., and this category is also protected by intellectual property rights.

Methods

Primary strategies for this exploration are engaging and relative techniques. A review article is a type of article that reviews the background of a scientific topic. In review articles, the results presented in scientific writings about a specific topic are summarized and evaluated. This type of article may examine anything, it is designed to summarize, analyze and evaluate information that has already been published. In such articles, experimental and new findings are rarely reported. Review articles have a well-defined narrative, are usually critical, and should provide theoretical and emerging interpretations. The important role of review articles is to guide original scientific writings. For this reason, it is essential that the citations provided are accurate and complete. They help to outline the issue acted like an entirety. Also, the technique of examination approaches permits us to see the primary patterns in the advancement of China's data strategy, to assess the different systems of China's unfamiliar digital arrangement drives, as well as to break down the possibilities for the improvement of data strategy regarding computerized discretion. The hypothetical and strategic reason for the review was the calculated place of logical examination in the field of concentrating on current worldwide relations. Utilizing the procedure of existing explores adds to a superior comprehension and inside and out investigation of the effect of worldwide digitalization on the political choices of the PRC.

Results and Discussion

The main purpose of this study is to analyze the current legislation of the People's Republic of China regarding information security. The article also describes the authorities involved in information security, and analyzes modern approaches to the study of information conflicts in domestic and foreign science. The scientific significance of this work is determined by the study of the most recent information conflicts, such as the conflict in Hong Kong, as well as the simultaneous analysis of the features of the information policy of the state.

The definition of state information security in China was derived by the Scientific and Technical Committee of the Central Military Council, one of the highest organs of the Communist Party of China. According to this definition, information security is the protection of four basic information processes – the collection of information, its processing, transmission, and storage – that is, the protection of information from illegal access. The definition also includes ensuring and supporting the use of information by its owner.

Information security according to the Chinese interpretation includes a decent level of awareness of potential threats, protection of information systems and infrastructure, security of information transmission and exchange, and control over its content [2]. Threats to information security from the point of view of the Chinese authorities come from three groups of factors: shortcomings in management in the field of information security, the risk of technical problems and hacker attacks [3].

The work of the Chinese authorities to ensure information security in the country began in 1994 with the publication of the first relevant state document. Let's list all the fundamental documents of the people's Republic of China in the field of information security:

1. "Rules of ensuring the security of computer and information systems" (1994) [4] gave rise to the control and inspection of state information security under the patronage of the Ministry of state security of the people's Republic of China. The document also provides for measures to work with crimes in the field of information technology.
2. “The State Informatization Plan and goals up to 2010” (1997) [5] was developed in order to identify the priorities of the Chinese government in the field of digitalization of public infrastructure.

3. “The law on network infrastructure and Internet security” of 1997 [6] supplemented the "Rules" of 1994 with a state ban on activities with certain types of information, for example, on the dissemination of information containing a call to violate state laws or terrorist propaganda.
4. “The Resolution on Internet security” [7] of 2000 stipulated the need for state control over information processes on the Internet due to the fact that China planned to widely use the Internet for state purposes (building economic and other infrastructure) and could not allow vulnerabilities in security systems.
5. “The Resolution of the State informatized steering group for work in the field of strengthening information security” [8] of 2003 approved the steps of the Chinese government towards comprehensive information security of structures of the most important state significance.
6. “The State strategy for the development of Informatization for the period from 2006 to 2020” [9] continued to apply the principles of the "Plan" of 1997, adding, among other things, the creation of regulatory bodies for information security, the development of national software.
7. “The decision of the State Council of the PRC on promotion of Informatization and development of the current protection of information security” 2012 [10] continued the principles of the above documents, going into detail and describing the rules of economic processes in the Network, as well as expanding the authority responsible for information security of power structures (for example, then the authorities of various levels were allowed to restrict public access to the Internet if necessary).
8. “The Anti-Terrorism Law of the People's Republic of China” in 2015 [11] gave even broader powers to information security agencies, allowing them to conduct extensive control over information coming from abroad, at their discretion to decrypt for terrorist propaganda or other prohibited information.
9. “The Cybersecurity Law” of 2016 [12] required Chinese users to use their real data when registering on various resources; in fact, it destroyed "fake" pages in social networks. Also, the law obliges the relevant authorities to keep all published information for 6 months.

   China, implementing its plans to improve information security and guided by the above-mentioned documents, has distributed responsibilities for ensuring information security among different sectors of government. In general, the problems of information security in the PRC are being addressed to:

   1. Central authorities of the CPC
   2. Government encryption management;
   3. Party and state leading groups, and small leading groups;
   4. National Security Committee;
   5. The People's Liberation Army (PLA);
   6. research and scientific institutions accountable to the state;
   7. PLA Academic institutes;
   8. Research centers.

It is additionally worth calling attention to that China takes global participation in the field of data security genuinely. At the drive and with the investment of individuals' Republic of China, numerous global archives connected with network protection have been embraced.

The "Procedure for global collaboration in the internet" - the principal official vital record on getting sorted out China's support in worldwide trade and participation in the field of global data security − was endorsed in Walk 2017. The Procedure calls for protecting sovereign correspondence (Web sway), repudiating authority on the Web, and declares non-obstruction in the interior undertakings of different states: "Since the primary part of present day worldwide relations, as per the UN Contract, is the rule of power... which likewise covers the internet. States should regard each other's more right than wrong to pick their own way of the internet improvement." "No nation ought to look for authority in the internet, meddle in the inward Undertakings of different States, or add to rebellious exercises in the internet" [13].

The archive likewise mirrors the standards of the UN Sanction, the arrangements of the SCO's Settlement on collaboration in the field of guaranteeing worldwide data security, the understanding between the Public authority of the Russian Organization and the public authority of individuals' Republic of China on participation in the field of guaranteeing global data security [14], of the draft Rules of lead in the field of guaranteeing global data security, the Ufa Statement of the VII BRICS Culmination in 2015 [15]. These lawful demonstrations approach states to appropriately follow the reasons and standards of the UN Contract, as well as lay out the guideline of legitimate arrangement of data security. Hence, the state energizes the advancement of organization foundation and specialized developments to create, streamline and further develop the data security of the Organization. As per the Methodology the accompanying objectives of the PRC to guarantee global data security are characterized: 1) assurance of Web sway, public safety and interests of China; 2) development of an arrangement of worldwide standards in the internet. 3) advancing reasonableness in Web administration; 4) safeguarding the authentic privileges and interests of residents; 5) advancing worldwide participation in the computerized economy; 6) making stages for the trading of cyberculture.

Summary

Information conflict in modern international relations is a complex and permanent phenomenon that is an integral part of international conflict [16, 18]. Information warfare, like any war, consists in achieving geopolitical goals and national interests by fighting, but not armed, but informational and informational-psychological, i.e. by influencing the information systems and processes of the enemy, as well as the consciousness of the mass population and individuals. The subjects of information warfare in modern international relations are primarily states and their unions, transnational corporations, international organizations, illegal radical formations and virtual social communities.

Since the 1990s, the People's Republic of China has been developing legislation and government structures responsible for information security. The priority is multi-level protection of state information resources, protection of the population from information and psychological impact, and increasing competitiveness in the global information market. Legislation and government structures are constantly evolving to meet global and regional information challenges.

The People's Republic of China is an active participant in international information conflicts. China has faced multiple attempts to interfere in internal Affairs from the outside [17], through information influence on the population and information systems. Currently available resources, structures and legislation allow it to prevent interference in internal Affairs, but some attacks, especially information and psychological attacks aimed at "demonizing" China in the eyes of the world community, are successful.

For the People's Republic of China, information security is a priority in foreign and domestic policy in the coming years. They are on the way to understanding the new "rules of the game", when information superiority is a key advantage in international relations. Comprehensive priority development of information technologies, information security systems, organizational and legal framework, as well as global media channels indicates that China is preparing for the fact that information warfare will occupy an even larger niche in international relations.

Conclusions

The People’s Republic of China, since the advent of the Internet in the country in 1987, has made far-reaching plans for how the Internet could help the Chinese authorities implement multiple projects for the "great revival of the Chinese nation". Ensuring information security in China is conducted carefully and sometimes quite rigidly, since the Chinese authorities do not intend to allow vulnerabilities in their information systems. China has also shown particular interest in consolidating information security standards at the international level through discussions at such venues as the UN, SCO, BRICS, and bilateral meetings of heads of state.

According to the law, doing some unauthorized activities in cyber space is a crime. As you know, there are different types of crimes in cyberspace and criminal actions can be carried out in this virtual network in many ways. Here we introduce some of the crimes that occur in cyberspace. According to Article 14 of the Computer Crimes Law and Paragraph 2 of Article 6 of the Press Law, publishing, distributing and trading vulgar and obscene content against public modesty in cyberspace is considered a crime, and the perpetrator must undergo legal punishment. Likewise, defamation is another offense that, if done, will result in punishment; The police warned people who defame and spread lies against each other in cyberspace and social networks that according to Article 17 of the Computer Crimes Law, by proving their criminal act, they should be accountable to the law and responsible for their criminal act.

Humiliating and insulting others in cyber space is a crime In addition to the mentioned cases, inciting, encouraging, persuading, threatening or inviting corruption and prostitution and committing crimes against chastity or sexual perversions are punishable according to paragraph b, article 15 of the Computer Crimes Law and article 639 of the Islamic Penal Code. Article 6, paragraph 2 of the press law talks about the spread of obscenity and obscenities, and this is also one of the criminal cases in the cyberspace, in addition to the instrumental use of people (both men and women) in images and content, humiliating and insulting women. Advertising illegitimate and illegal rituals and luxuries is also considered a crime. If disruption of national unity and creating differences between social strata occurs in the cyber space, especially through raising racial issues, the perpetrator is guilty and must be held accountable for his criminal act.

Acknowledgements

This paper has been supported by the Kazan Federal University Strategic Academic Leadership Program.

Bibliography

[1] D.A Balakin, A.R Alikberova, E.K Khabibullina. Information policy of the People's Republic of China in Xinjiang-Uyghur autonomous region. Opcion, 2019. Vol.35, Is.Special Issue 22. P.410-421

[2] Report of the Scientific and Technical Committee of the CPC CPC. The official website of the Ministry of Defense of the PRC. [Electronic resource]. - URL: http://www.mod.gov.cn/jmsd/2018-08/17/content_4822760.htm (accessed: 05.15.2020).
[3] The official website of the Permanent Mission of the PRC to the UN. [Electronic resource]. - URL: (https://www.fmprc.gov.cn/ce/ceun/chn/zgylhg/jjalh/alhzh/fnhpaq/t1607577.htm (accessed: 05.15.2020).
[4] Regulation rules ensuring the security of computer and information systems. The official website of the China Internet Information Center. [Electronic resource]. - URL: http://russian.china.org.cn/links/txt/2007-09/28/content_8978975.htm (accessed: 05.15.2020).
[5] The situation of the Internet in China. The official website of the China Internet Information Center. [Electronic resource]. - URL: http://russian.china.org.cn/government/archive/baipishu/txt/2011-02/01/content_21857458_2.htm (accessed: 05.15.2020).
[6] Law on the security of network infrastructure and the Internet. [Electronic resource]. - URL: https://baike.baidu.com/item/ 互 (accessed date: 05/15/2020).
[7] Organizational and legal support of information security: Textbook and workshop for undergraduate and graduate studies / Ed. T.A. Polyakova, A.A. Streltsova. M., 2016.S. 136.
[8] Decision of the state informatized steering group for work in the field of strengthening information security. [Electronic resource]. - URL: https://wenku.baidu.com/view/bdfba07271fe910ef02df886.html (accessed: 05.15.2020).
[9] State strategy for the development of informatization for the period from 2006 to 2020 [Electronic resource]. - URL: https://baike.baidu.com/item/2006-2020 (accessed: 05.15.2020).
[10] Decree of the State Council of the PRC on the promotion of informatization and the development of the existing protection of information security. [Electronic resource]. - URL: http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm (accessed: 05/15/2020).
[11] Antiterrorist Law of the PRC. [Electronic resource]. - URL: https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85 %B1%E5%92% 8C% E5% 9B% BD% E5% 8F% 8D% E6% 81% 90% E6% 80% 96% E4% B8% BB% E4% B9% 89% E6% B3% 95/15954871? Fr = aladdin (accessed: 05/15/2020).
[12] PRC Law on Cybersecurity. [Electronic resource]. - URL: https://baike.baidu.com/item/ 中华人民共和国 网络 安全 法 / 16843044? Fr = aladdin (accessed: 05.15.2020).
[13] SCO Agreement on Cooperation in the Field of International Information Security of June 16, 2009 (Entered into force on January 5, 2012) [Electronic resource] URL: http://docs.cntd.ru/document/902289626 (accessed: 04/21/2020)
[14] Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of international information security of 05/08/2015 [Electronic resource] URL: http://www.mid.ru/en/maps/cn/-/asset_publisher / WhKWb5DVBqKA / content / id / 1257295 (accessed: 04/21/2020)
[15] Ufa Declaration of the VII BRICS Summit of July 9, 2015. [Electronic resource] URL: http://static.kremlin.ru/media/events/files/ru/YukPLgicg4mqAQIy7JRB1HgePZrMP2w5.pdf (accessed: 04/21/2020)
[16] Szafranski R.A. Theory of Information Warfare: Preparing for 2020 // Airpower Journal. Spring 1995; - 412 p.
[17] Hughes R. China Uighurs: crackdown. [Electronic resource] // BBC News, 08.11.2018. Available at: https://www.bbc.com/news/world-asia-china-45474279 (accessed: 10.02.2019).
[18] Ilikova L.E.,,Svirina A. Social protests in 2011: International perspective and information access International Journal of Criminology and Sociology Vol. 9, 2020, pp 994 - 996