Orientation Research of Network Security Management in China

Daoli Huang[1,2, a, *] Hao Yuan[3,b] Zhile He[2,c]

[1] Xi`an Jiaotong University,Shanxi,China

[2] Key Laboratory of the Ministry of Public Security of Information Network Security,

The Third Research Institute of the Ministry of Public Security, shanghai, China

[3]Jiangsu Zhuhui Law Office, Jiangsu, China

[a]email: huangdaoli@stars.org.cn

[b] email: 13701414840@163.com

[c]email: hezhile@stars.org.cn

Keywords: Information security; Legal concept; Overall national security concept; orientation

Abstract: Information security has gone beyond the traditional scope of information communication and media, become the key related to the core interests of China's national security, social stability and personal privacy, etc. Establishment of a comprehensive network and information security management system has become the urgent priority, thus accelerating the legislation of network and information security in our country is pressing. The purpose of the legislation of network and information security in our country should lie in combating the threats from network information security, promoting the industrial development, safeguarding national security and social stability, and protecting the legitimate interests and rights of related parties. We should take the "information security" as the object of legislation, "the overall national security concept" as the concept to guide the stipulation of comprehensive legislation, and build the trinity frame of the network and information security management legal system featuring "defense, control and punishment".

At present, China's national security and social stability face unprecedented information security threats. February 27, 2014 Central Network Security and Information Leading Group was formally established, indicating that China will enhance the network security up to the height of national security, and the establishment of a comprehensive network and information security management system has become the urgent priority. Legal governance is one of the important components of network and information security governance，with the force of law it maintains the normal order of the network space and safeguards the security of national critical information infrastructure. The National People's Congress has put the network safety into their legislation plans in 2014. Some researchers proposed building a legal system of network and information security governance with the harmful information management as the core, there are also some researchers considered building a legal system of network and information security governance from the perspective of criminal law. This text discusses the legislation orientation problem of China’s network and information security from the perspective of concept interpretation, legal governance and governance system.

Concept Interpretation: the relationship between information security and network security

In China, the concept and use of information security, network security has always been controversial. From the actual use, information security, English as "Information security", has been widely used in existing policies and legislation documents at home and abroad; network security, has developed to be the meaning of "cyberspace security" (English as "Cyberspace security" or Cybersecurity") 1from a purely technical terms (English as "Network security")1,the use of it witnesses a huge increase in the new policy and legislation documents at home and abroad. Some

[1] The network security in this article also adapts the new meaning of "Cyberspace security" or Cybersecurity ".

researchers recommend bypassing this controversy with specific legislation work. But the concept is a reflection of the essential attribute of things, the basic element of legal thinking, grasping the extension of concept can better define the scope of the object that the concept referred to. [1] Cybersecurity legislation, the primary task, we might start from the definition of the concept. [2]

From the time of the 911 incident up till present, the national critical infrastructure is increasingly dependent on information systems ,the dependent features of cyberspace security are becoming more obvious , network security ("Cyberspace security" or "Cybersecurity") has become the key related to the core interests of China's national security, social stability and personal privacy ,etc, cyberspace safeguard has become an important area of national power competition, countries have begun to actively adjust the national strategy of Cyberspace security to information security legislation. In the use of information security and network security terms, the EU and the United States have started to reflect the difference. The EU takes network and information security as a whole, and related regulations, decisions and resolutions in the legal documents has always used the "network" and "information security" together. “The European Parliament and the EU Council No. 460/2004 Regulation about the establishment of European Network and Information Security Agency" clearly states, "network and information security" indicate the ability of resisting accidents, illegal and malicious behaviors that the network or information systems have ,the purpose of these illegal and malicious behaviors is trying to undermine the availability, authenticity, integrity and confidentiality of the data and related services stored or transferred in the network and system.2 U.S. legislation documents continue to follow the information security concept in the "Federal Information Security Management Act" [3], while take the "Information security", "Cyberspace security" and "Cybersecurity" as synonyms to use interchangeably. On the definition about "Cyberspace security" and "Cybersecurity", in 2003 the United States' national security strategy for cyberspace "points out, Cyberspace is the " nervous system " that ensure the country's critical infrastructure operating normally ,and is the country's control system .The recent study of IT research and consulting firm Gartner thinks , Cyberspace is the concept used by the U.S. military for 10 years ,it refers to the governance, development, management and use on the information security technology, operation and control technology, IT security tools and techniques in order to obtain compliance, protecting assets, attacking rival assets. Meanwhile this definition emphasizes the concept of defense and attack, with a clear national interest color. In the International Standard ISO / IEC 27032: 2012 "Information technology - Security technology - Cyberspace Security Guide", "Cybersecurity" and "Cyberspace security" are equivalently defined , define the cyber(space) information security around the core attributes of information security, defined as "protecting the confidentiality, integrity ,usability and other attributes, such as Authenticity, confirmation, non repudiation and reliability of the information in cyberspace. "[4]

In the definition of the relationship between information security and network security, the provisions of international standard ISO / IEC 27032: 2012 are more reasonable ,and worthy of reference for us. The standard states that "cyberspace security relies on information security, application security, network security andinternet security and other domains, but not equal to these security areas." ISO / IEC 27032: 2012 uses the figure to express the relationship between cybersecurity and other security domains, the "National Cyber Security Handbook" issued by the NATO cyber defense center of excellence in 2013 adopted the viewpoint of ISO / IEC 27032, in which uses a similar figure to define the relationship between cybersecurity and other security domains.

[2] From the perspective of legislation orientation ,the definition of EU seizes the "information network" that is the key link of contemporary Information Security, notices the requirements of being engaged in related services through the information system, establishes the definition of information security above the certain security trust level, and thus proposes the requirements of "capacity", this is more favorable to grasp the adjustment range of information security activities from the legal .

Through comparing the two figures we can see that, the scope of "Information security" is bigger than that of "Cybersecurity". the focus that both emphasize is different, the focus that "Information security" emphasizes is the data security, is not limited to any media, including supply chain, network application, critical infrastructure and Internet services ,etc. "Cybersecurity" focus on critical infrastructure (such as energy, telecommunication, and water authorities) and the security of supply chain.

In summary, we can see that, although the concepts of information security and network security are different, the use in legislation documents of different countries are not the same, but their essences are safeguarding the safety, promoting social development and maintaining economic prosperity. Currently, network security has become the cornerstone of the country's economic development, the cornerstone of national security and social stability, China's Network Security and Information Leading Group has clearly raised that network and information is " the two wings of one, the two wheels of one driver," it is necessary to solve our network security issues, but also to promote the development of information, thus solve security issues in the information construction. In such cases, emphasizing the information security in a broader meaning better conform to the reality that our country is a developing country, using the concept of "information security" is a natural and reasonable choice. Therefore, this article believes that the object of the legislation in our country at present should be "information security" instead of "network security", in order to limit the scope of information, we can learn from the regulations of EU, which use the "Network and Information Security Law" or "Network Information Security Law ".

Legal concept: the overall national security concept

"The supreme principle of law-making and application, is called legal concept; the legal concept, is the guiding principle of the law purpose and means." [5] In the law philosophy view, legal concept is a kind of broader overall rational cognition and grasp on the nature of law and its law of development. The level of legal concept is higher than the level of legal idea, legal notion and legal awareness; it can conduct scientific prediction and guidance to the legislation and implementation of laws. Legal concept of modern law includes justice, democracy, equality, the rule of law, rights, safety, efficiency and sustainability, etc. The value and effect of Security concept as universal human basic needs have been constantly highlighted.

With the constant development of network information technology, our nation's critical infrastructure is increasingly dependent on the complex cyberspace, in the first meeting of the National Security Committee, President Jinping Xi pointed out that, " connotation and extension of our national security at current are richer than that of any time in history, temporal and spatial domains are wider than that of any time in history, internal and external factors are more complex than that of any time in history "[6] Any damage in the cyberspace has a huge impact on national security and social stability. With a pragmatic view, President Jinping Xi, proposed the new idea of "insist the overall concept of national security, explore the road of national security with Chinese characteristics," emphasized nation’s safety development should take the internal and external security, homeland and national, traditional and non-traditional, the safe development, self and mutual security into account. "The overall concept of national security," stressed the deeper, higher and more comprehensive integrated security, creatively proposed the values, work ideas and mechanism path on national security with Chinese characteristics, it is a rational cognition that is broader and more comprehensive than the "security concept" or "comprehensive security concept ".

The overall national security concept" provides scientific guidance for the formulation and implementation of the network and information security legislation in our country, the network security that conforms to the requirement of "the overall national security concept" is the network security under an open environment at home and abroad, not fragmented, localized and territorialized

network security. We should establish the legal concept of "the overall national security concept ", formulate and implement the comprehensive legislation of "the overall national security concept".

First of all, our country urgently needs a comprehensive legislation to guide the development of information. President Jinping Xi at the first meeting of the central network security and information leading group emphasizes, "network security and information is a major strategic issue related to the national security and national development, and the people‘s life, we should take the international and domestic situation as the starting point, overall layout, co-ordinate the parties, innovate the development and make great efforts to build our country into the network powerful nation." This top-level deployment cannot only be turned into a national industrial promotion law, internet information content management law or criminal law. Only through the comprehensive legislation, clarifying the country’s basic principle of network information security, unifying deployment planning and establishing the comprehensive legal system of public opinion monitoring, emergency response, technical personnel and organic safeguards, etc on national network information security , only in this way can we implement the concept of "overall national security concept" ,reflect the central strategic requirements on the development of network security and information and achieve the whole security purpose of national security, social stability, industrial development and the protection of personal privacy.

Second, formulating a comprehensive legislation conforms to international practices. The informationalized developed countries have long recognized that the network security is one of the important problems that threaten the national security, have scrambled to formulate the comprehensive legislation to regulate. American has formulated the "Patriot Act" in 2001, "the Federal Information Security Management Act" in 2002, "homeland security Act" in 2002 and other laws, that specify the contents about the network monitoring, governmental information protection and national security, etc.. Although since 2009 American’s network security act suffered a setback, but in the area of network information security it has formed the tangles of legal system. "The No. 92/242/EEC decision on information system security domain of EU Council in March 31, 1992 " clearly points out that the action plan used to safeguard the information system’s security includes formulating a unified strategic framework of information system security ", and avoiding the fragmented countermeasures damaging the effect of Information Security Legislation". This provision had a profound impact on the formulation of the EU’s legal policy on information security. "In 2006 the EU Council’s suggestion about formulating, recognizing and appointing the European critical infrastructure, and evaluating the instruction of the necessity of improving the protection " also belongs to the comprehensive legislation. As a developing country, in 2000 India enacted a comprehensive legislation law named " information technology law”, it regulates digital signature, electronic government, administration, criminal prosecution and other contents, in 2008 and 2011 this law was revised twice to perfect gradually.

Again, formulating the comprehensive legislation conforms to the legislation requirements of our country’s reality. The legislation of network and information security covers a wide demand, and is closely related with the rapid combination of new technologies and new applications such as cloud computing, mobile internet and intelligent terminals, etc. China's current laws and regulations about the information security involve multiple levels of laws ,administrative regulations, departmental rules and regulations, local regulations and normative documents ,etc, on longitudinal the content they covers includes the information security and criminal sanctions of information security in the specific domains such as the network and information system security, information content security, information security systems and products, secrecy and password management, and computer virus prevention, in the vertical the content includes the maintenance of governmental information security, the safeguard of the enterprises’ rights and the protection of personal information rights. But on the whole, current laws and regulations can not effectively deal with the increasingly serious threats of information security. The Prism Scandal exposed the legal safeguard on the maintenance of national data sovereignty and national industrial revitalization is insufficient; the legal system about national

critical information infrastructure such as telecommunications, electricity, transportation and banking securities, etc is not perfect, the policy and law safeguard of technology research and product development on the information security is weak ,when the major incident, circumstance and state of emergency happen, the emergency response lacks of legal safeguard, emergency plans, criminal information and security testing that can be used as the information of social security precaution ,this information is difficult to share, and seriously affects the capability of rapid response, security safeguard and coordination. Aiming at this situation and the actuality, the interpretation, revision or supplement of the laws previously, can't grasp the relationship between security and development, thus against achieving the goal of the national overall security strategy.[7] China should formulate the comprehensive legislation, clearly defines the baseline of network and information security, thus provides a legal basis for the departmental ,local legislation and the policy's formulation, adjustment and improvement.

Governance system: defense, control and punishment

Governance refers to under the support of network technology as the representative of the information technology, the government, non-governmental organizations, businesses, individual citizens and other social diverse elements involve in cooperation and coordination , aiming at the potential and the current crisis, in the different stages of crisis development a series of control actions should be taken to effectively prevent, process and eliminate the crisis, and ultimately achieve the purpose of maintaining and promoting the public interest to the best. President Xi Jinping proposed that we must "rule the cyberspace by law," building the legal system of network and information security governance that reflects China's national conditions and interests is the foundation. This article thinks that we should establish the trinity frame of governance legal system featuring "defense, control and punishment" ,use the "defensive and controlled" legal norms instead of the traditional pure "punitive" criminal legal norms, from the level of multiple subjects participating in the comprehensive governance clearly define the process control requirements of multiple subjects during the early warning and monitoring, emergency and response of the information security incidents,control and recovery ,etc to defense, control, reasonably distribute the security risk and punish the illegal crime and terrorist activities in the cyberspace .

"Defense" in this article means the "active defense". "The National Information Leading Group's opinion on strengthening the safeguard work of information security " (No. [2003]27 article) and "from 2006 to 2020 the development strategy of national information " both clearly confirm the active defense is the national information security strategic policy. The global characteristic of information security threat determines that the information security risk exists in the whole process of information security , the implementation of active defense helps strengthen the national control over the information security risk. The principle of active defense in the legislation, refers to all kinds of technical measures what the country should take in the process of network and information security to improve all management systems, standardize the education of information security , pay attention to the relationship between the technology, management, the society, economy and the law in the information security activities, prevent all kinds of security risks in the process of national information construction with the law enforcement,in the meanwhile, implement strategic deterrence and effective suppression for the attack source that has been defined. [8]The legislation of the network and information security that takes the active defense as the principle, will take the initiative to build the legal governance capacity of the information security from all links of finding threat, reducing risk and controlling risk, for example, in the aspects of content security control, while focus on sealing , pay more attention to promote the development of the network through the management and guidance ;in the promotion of technological and industrial development , fully emphasize developing the leading effect of the government, from the pre-funding support changes to the later procurement support, protect the huge domestic market and support the development of national

industry through the procurement policies; on the aspect of building the emergency processing mechanism , pay attention to the advance warning, risk prevention and social mobilization in emergency circumstances.

"Control" in the legal norm's form is more a procedural legal norm, it is used to clarify how to implement the responsibility, how to exercise their rights and fulfill their obligations, how to combat criminals and terrorists. Current laws tend to emphasize the substantive legal norms, that results in the difficulty of implementing substantive rights and obligatory norms . The establishment of network security procedural legal norm is an inevitable choice to protect the network security , other countries in the world have paid attention to this situation, for example, although American "easy health insurance liability law" was issued in 1996, but in 2003 the Ministry of Health and Public Services issued guidelines to safeguard information security, further clarified the procedural provisions how to safeguard information security from three aspects of physics, technology and management. The relevant resolutions of the Economic Cooperation Organization on network security's cultural guideline and the United Nations also put forward countermeasure about the control process of network security.[9]

"The punishment is a kind of remedial legal norms that is mandatory and focusing on the results identification. It uses the substantive criminal law more as the main adjustment method. At the present stage our country's network crime and terrorism showed the new rising trend, ways and forms. The ineffective punishment means indulging the crime, the effect of prevention and control is difficult to implement. The punishment is irreplaceable in the legal system of governance, with the dual effect of punishment and deterrent, On the one hand, punishing illegal and criminal acts, on the other hand, having the deterrent effect on potential illegal behavior. Strengthening against the network crimes is a consensus within the international community, EU's "Cybercrime Convention "in 2001 builds a set of minimum international standards to punish network crime. In 2013 the EU issued the "2013/40/EU directive about attacking information system (" instead of "No. 2005/222/JHA framework decision about attacking information system "in 2005), emphasized that the EU needs to enhance protective capability of critical infrastructure, the measures against cyber attack should show serve criminal penalties.[10]

Suggestion and Conclusion

This article thinks that, establishing and improving the trinity frame of network and information security governance legal system featuring "defense, control and punishment" can include the following contents: clarify management and decision-making mechanism. The working mechanism of the central network security and Information Leading Group Office should be clarified; regulatory institutions and their responsibilities should also be clarified .An independent regulator of information security should be set up, the scope of official duties of the institutions such as public security, confidentiality, national security, industry and information, communication and business secret management, etc should be refined and clarified, or in accordance with the function expansion implement the supervision and management in the scope of original authority; clarify the protection system of critical information infrastructure. The legislation principle of critical information infrastructure protection, should be established, the organizational system and working mechanism of critical information infrastructure protection should be clarified, the monitoring reporting and early warning mechanism, emergency response and response recovery mechanism, security supervision system and accountability system of critical information infrastructure protection should be built; clarify communication security system. The rrequirements of communication security should be clarified, the guarantee mechanism of communication security should be set up, to regulate the use of instant communication, VOIP, e-mail and other modern communication technology, and ensure the freedom of communication and national security. The legal system which prevents the abuse of attack, intrusion, malicious programs and other information technology, should be built to

safeguard the security of communication and other information systems and data security, and to prevent from unauthorized accessing, using, interrupting and revealing the computer's information resources; improve the management system of Internet information services.

The "management approach of internet information services " in 2000 needs to be modified, whose content can include the ISP, ICP security protection obligation, especially the security protection obligation about the collection and usage of consumer's data, the standard of identifying internet terrorist and other illegal harmful information should be clarified, the retention period of communication data should also be clarified; clarify the review system of national information security. The scope and standard of information security review should be clarified, we should implement a comprehensive review on the network information infrastructure, products and service, examine the security of the information security products and services that are purchased and arranged by the key departments and important areas, regularly examine the guarantee measures of information security in the key business areas and examine the reliability and controllability of the information security products and services that import from abroad; clarify network monitoring system. We should regulate the conditions and procedures of communication interception technology used by the legal operation department in handling criminal cases, clarify the duties of enterprises, other organizations and citizens to assist a law enforcement ; clarify the judicial cooperation mechanism of cross-border data flow, we should regulate the international major crimes , terrorism intelligence-gathering activity and other activities; clarify the provision on army's network information security legislation .

Acknowledgements

In this paper, the research was sponsored by the Shanghai science and technology commission project: legal measures and standard specification research of personal data protection in big data environment (Project Number: 13511504100).

References

[1] Minhu Ma: *Research on Information Security Law*(Shanxi People's Press, 2004),p.20(In Chinese).

[2] Chinese Network Security Legislation in an complex and open environment on http://www.chinais.net/portal.php?mod=view&aid=5627.

[3] Shi Yuchun; Li CzhangXi and Wei Zaixue: criminal responsibility of Illegally obtain communication customer's personal information.Journal of Beijing University of Posts and Telecommunications (Social Science Edition),january,2010 (In Chinese).

[4] ISO / IEC27032: Information technology -Security techniques -Guidelines for cybersecurity, First edition .

[5] Shi Shangkuan:*the Synthesis of Law Concept and Empiricism Jurisprudence* (Taiwan Hanlin Press, 1984),p. 259 -260(In Chinese).

[6] Jinping Xi: adhere to the national overall security concept and go the national security road with Chinese characteristics on http://news.xinhuanet.com/2014-04/15/c_1110253910.htm.

[7] Minhu Ma: Network Security: Legal confusion and countermeasures,Journal of Chinese People's Public Security University (Social Science Edition), issue1,2007(In Chinese).

[8] Min Hu Ma; Wang Lei:The thinking of constructing our country's information security legal capacity. Information Network Security .October, p.27 (In Chinese).

[9] Minhu Ma:*Research on Information Security Law* (Shanxi People's Press, 2004).p.3.(In Chinese).

[10] On the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA On http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2013-224&language=EN.