ON THE CRIMINAL REGULATION OF CRITICAL INFORMATION INFRASTRUCTURE FROM THE PERSPECTIVE OF INTERNATIONAL LAW

LIXIN ZHU[1] RUOLIN ZHANG[2] YUE MA[3]

I. INTRODUCTION

Critical Information Infrastructure (CII) is the basic layer of the Internet, and its safe and continuous operation is the basis of network security.[4] In recent years, crimes against critical information infrastructure have become more frequent and present a trend of transnational attacks. International cooperation to protect critical information infrastructure and jointly manage cyberspace crimes has become the best way to solve this international problem. In this governance process, international law principles, norms or maxims that have been widely recognized or formed should be respected. They are also the basic platform for cooperation and construction of governance models. International law principles such as the Charter of the United Nations, the Five Principles of Peaceful Coexistence, and other international legal norms also provide ideas and a basic normative framework for network governance.[5] Therefore, the best choice to solve the problem is to construct a win-win network security global community of common destiny, and to regulate the crime of Critical Information Infrastructure from the perspective of international law.

[1] Doctor of Law, Postdoctoral in Management Science and Engineering, Associate Professor, Executive Director of Suzhou Institute of Information Security Law, Vice President of Shaanxi Branch of China Information Security Law Society.

[2] PhD candidate at Law School of Xi ‘an Jiaotong University (majoring in network security law).

[3] Works at Xi ‘an Power Supply Company of State Grid Shaanxi Electric Power Company.

[4] Chen Yuefeng, *Cooperative Governance of Critical Information Infrastructure Protection*, 6 CHINESE J.L. 175 (2018).

[5] Xu Longdi & Lang Ping, *Basic Principles of the International Governance on Cyberspace*, 2018 INT’L REV. 33.

II. THE HARMFULNESS OF CRITICAL INFORMATION INFRASTRUCTURE CRIMES

In early April 2018, the African Coast-Europe (ACE) submarine cable was cut, disrupting access to parts of Sierra Leone and the national network of Mauritania, which went "offline" for two full days.[6] Attacks on the power grid become even more frequent. Venezuela's persistent power cuts in recent years have taken a huge toll on the country.[7] Venezuela's blackout is not the first time a critical information infrastructure has been attacked with a significant impact. Other similar incidents include Iran's Stuxnet and Ukraine's power grid blackout. From Iran to Ukraine to Venezuela, cyber attacks on a country's critical information infrastructure have become an important issue in terms of cyber crime, cyber attack and defense.

China's National Cyberspace Security Strategy, released in December 2016, pointed out that

> Networks and information systems have become critical infrastructure and even nerve centres for the entire economy and economic society.When they suffer from attacks and destruction, or major security incidents occur, it will lead to paralysis of critical energy, transportation, telecommunication and financial communication, finance infrastructure, etc., resulting in disastrous consequences and gravely harming national economic security and the public interest.[8]

Information security is facing a complex and severe situation. Once security problems occur in basic information networks and important information systems, they will directly threaten national security, social stability and economic development. In response to this transnational

[6] *See* Russell Brandom, *A Broken Submarine Cable Knocked a Country off the Internet for Two Days*, VERGE (Apr. 8, 2018, 3:00 PM), https://www.theverge.com/2018/4/8/17207556/submarine-internet-cable-mauritania-broken.

[7] The most serious of a continuous nationwide large-scale blackout has affected the capital, Caracas, and at least twenty of the country's twenty-three states, affecting nearly thirty million people. Venezuelan President Maduro claimed that the power outage was a cyber attack, targeting the Simon Bolivar hydroelectric power station and its connected Caracas control center. *Venezuela power cuts: Blackouts hit Caracas and spread*, BBC (Mar. 8, 2019) https://www.bbc.com/news/world-latin-america-47492624.

[8] *National Cyberspace Security Strategy*, CHINA COPYWRITE & MEDIA (Dec. 27, 2016), https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/. The document clarifies China's major position on the development and security of cyberspace, and its role is to guide China's cybersecurity work and safeguard the country's sovereignty, security, and development interests in cyberspace. *Id.*

challenge and extremely serious social problem, the international community has begun its efforts to sanction international crimes.

III. INTERNATIONAL CRIMES RELATED TO CII – THE LEGAL BASIS FOR CII INTERNATIONAL COOPERATION

From the perspective of international law, our research proposes that CII related international crimes can be divided into two categories: "Wartime" and "Peacetime." "Wartime" includes crimes of violating peace, war crimes and crimes against humanity. "Peacetime" includes terrorist crimes and computer crimes.[9] The consensus of the international community on these criminal acts is the legal basis for international cooperation to protect CII.

There are international crimes related to CII in wartime:

1. Crimes Against Peace refers to the criminal act of planning, preparing, launching or carrying out an aggressive war, including the threat or use of force against the territorial integrity or political independence of any country, or any other network action that is inconsistent with the purpose of the United Nations.[10] The United Nations Charter also has related prohibitions.[11] Therefore, if the scale and consequences of cyber operations against CII reach a certain level, CII attacks may constitute crimes against peace.

[9] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

[10] After World War II, the Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, and its annex the Charter of the International Military Tribunal, established the crime of breaching peace as a war crime. Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, Aug. 8, 1945, 82 U.N.T.S. 279; Charter of the International Military Tribunal—Annex to the Agreement for the prosecution and punishment of the major war criminals of the European Axis, Aug. 8, 1945, 82 U.N.T.S. 284 [hereinafter European International Military Tribunal]. The European International Military Tribunal and the Charter of the International Military Tribunal of the Far East listed the "crime against peace" as the first war crime within the jurisdiction of the court. European International Military Tribunal, *supra*, at 288; Charter of the International Military Tribunal for the Far East art. 5(a), Jan. 19, 1946, T.I.A.S. No. 1589 [hereinafter Far East Military Tribunal]. In 1970, the United Nations General Assembly adopted the *Declaration on Principles of International Law* and reaffirmed that countries should resolve international disputes with other countries by peaceful means to avoid endangering international peace, security and justice. G.A. Res. 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations (Oct. 24, 1970). According to the Declaration, responsibilities for wars of aggression and endangering the peace must be clearly defined, and those who prepare or initiate illegal wars should be held accountable. *Id*.

[11] U.N. Charter art. 2, ¶¶ 3–4 ("All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

2. War Crimes refers to the criminal acts that violate the laws and customs, including maltreating or killing prisoners, hostages, laborers, plundering property and destroying cities and towns. It also includes cyber attacks that do not target legitimate targets, as well as unrestricted attacks against legitimate targets and civilians or civilian objects.[12] It is difficult to distinguish between civilian targets and military targets for CII attacks. Therefore, a CII attack is very likely to constitute an indiscriminate war crime.

3. Crimes Against Humanity can occur before and during war and refers to the killing, extermination, enslavement and other inhumane acts of any civilian, including causing excessive harm or unnecessary suffering.[13] In addition, international law also prohibits starvation of civilians as a method of cyber warfare, and prohibits the use of cyber operations to engage in retaliation against the following objects: (1) prisoners of war; (2) detained civilians; (3) people who have lost combat effectiveness; (4) medical personnel, equipment, transportation vehicles.[14] If a cyber attack on CII confines civilians to starvation, or actually leads to retaliation against the above four categories of objects, it may also constitute a crime against humanity.

[12] The International Law Commission ("ILC") drafted the Rome Statute in 1998, pointing out that a war crime is an objective and specific act in violation of relevant specific laws and customs of war. Rome Statute of the International Criminal Court, art. 8, July 17, 1998, 2187 U.N.T.S. 90. These relevant laws, including *Geneva Convention* and the *Declaration on the Protection of Women and Children in Emergency and Armed Conflict*, stipulate the manifestations of war crimes. *See generally* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 75 U.N.T.S. 31; G.A. Res. 3318 (XXIX), Declaration on the Protection of Women and Children, arts. 1, 2, 4–5 (Dec. 14, 1974).

[13] The European International Military Tribunal and the Far East International Military Tribunal stipulate that a crime against humanity refers to the murder, annihilation, enslavement, exile, and any other inhumane acts of civilians before or during war, or abuse based on political, ethnic or religious reasons. European International Military Tribunal, *supra* note 10, art. 6(c); Far East International Military Tribunal, *supra* note 10, art 5(c). The Rome Statute also has similar provisions. Rome Statute, *supra* note 12, art. 7.

[14] *See* Rules Concerning the Control of Wireless Telegraphy in

Time of War and Air Warfare (Dec. 1922-Feb. 1923) *in* DOCUMENTS ON THE LAWS OF WAR 139 (Adam Roberts and Richard Guelff ed.s, 2000); Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Yves Sandoz et al. ed.s, 1987); Customary International Humanitarian Law (Jean-Marie Henckaerts and Louise Doswald-Beck ed.s, 2005); Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (Jean Pictet ed., 1952); Commentary on the Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949 (Jean Pictet ed., 1960); Commentary on the Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Jean Pictet ed, 1958).

There are the international crimes related to CII in peacetime:

1. Computer Crimes under the Convention on Cybercrime.[15] In order to combat transnational crime, in November 2001, the 26 European Union member states of the European Commission and government officials from 30 countries including the United States, Canada, Japan and South Africa signed the Convention on Cybercrime in Budapest.[16] The Convention on Cybercrime became the world's first international convention against cyber crime; it also has a series of relevant regulations concerning crimes against CII.[17] The Convention on Cybercrime also specifies the general principles[18] of international cooperation, which has played an important guiding role in our cooperation in combating cyber crime.

2. Terrorism Crime. After 9/11, international legislation on terrorist crimes was strengthened. Attacks on critical information infrastructure constitutes terrorist acts and are penalized by relevant laws against terrorism. Numerous legal documents[19] indicate that cyber attacks on CII constitute terrorist crimes and violate a country's domestic criminal laws, thereby further triggering international criminal cooperation against terrorist crimes. For example, on June 15, 2001, six countries signed the Shanghai Convention on Combating Terrorism, Separatism and Extremism.[20] At the 12th ASEAN Summit in 2007, ASEAN countries

[15] Convention on Cybercrime, Nov. 23, 2001, S. Treaty Doc. No. 108-11 (2003), 185 E.T.S. 1.

[16] *Id.*

[17] The criminal provisions relating to CII include: Article 2, Illegal Access; Article 3, Illegal Interception; Article 4, Data Interference; Article 5, System Interference; Article 7, Computer related forgery; Article 8, Computer related fraud. Convention on Cybercrime, *supra* note 15, arts. 2–5, 7–8.

[18] The general principles relating to international co-operation are as follows: "[t]he Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence." Convention on Cybercrime, *supra* note 15, art. 23.

[19] *See, e.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001); *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, COM (2006) 786 final (Dec. 12, 2006); Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN), COM (2008) 676 final (Dec. 27, 2008); NAT'L SEC. COORDINATION CTR., THE FIGHT AGAINST TERROR: SINGAPORE'S NATIONAL SECURITY STRATEGY (2004), https://www.files.ethz.ch/isn/156810/Singapore-2004.pdf .

[20] Shanghai Convention on Combating Terrorism, Separatism and Extremism, June 15, 2001., U.N. INT'L INSTRUMENTS RELATED TO THE PREVENTION AND SUPPRESSION OF INT'L TERRORISM, at 232–40, U.N. Sales No. E.08V.2 (2008). This document was jointly signed by six countries, together forming the Shanghai Cooperation Organization ("SCO"), include the Republic of Kazakhstan, the people's Republic of China, the Kyrgyz Republic, the Russian Federation, the Republic of Tajikistan and the Republic of Uzbekistan. *Id.* at 232.

signed a legally binding document in the region – the ASEAN Convention on Counter-Terrorism.[21] These international conventions against terrorism have laid the foundation of international law for international cooperation in combating terrorist crimes against CII.

IV. CII COOPERATION STRATEGIES OF MAJOR COUNTRIES – THE POLITICAL BASIS FOR CII INTERNATIONAL COOPERATION

The interconnectedness and globalization of networks has presented cybersecurity issues with the protection of critical infrastructure, which is the core challenge faced by all countries in the world today. In this context, international organizations and many countries have always paid attention to the construction of national critical infrastructure and critical information infrastructure protection strategies, legislation and organizational systems.[22] Countries have similar strategic intentions for the protection of critical information infrastructure, and all emphasize the importance of protecting critical infrastructure through international cooperation.[23] At the same time, major countries have established a system of priority protection for critical infrastructure in legislation and adopted periodic protection measures. Based on the past experience in international criminal crime cooperation, these joint measures have laid the foundation for international cooperation in the protection of critical information infrastructure.

[21]ASEAN Convention on Counter Terrorism, Jan. 13, 2007, https://asean.org/?static_post=asean-convention-on-counter-terrorism. Prior to this, ASEAN and the United States, China, Japan, Russia, Australia, India, Canada, New Zealand, Pakistan, the European Union and other countries or organizations also signed anti-terrorism cooperation declarations or agreements.

[22] Elgin M. Brunner & Manuel Suter, INTERNATIONAL CIIP HANDBOOK 2008/2009, at 296–300 (Andreas Wenger, Victor Mauer & Myriam Dunn Cavelty eds., 4th ed. 2008).

[23] In recent years, the signing of many international cooperation agreements in the field of cybersecurity, such as the The Paris Call for Trust and Security in Cyberspace, shows the intention of countries to cooperate in the governance of cyberspace. *Paris Call for Trust and Security in Cyberspace* (Nov. 12, 2018), https://pariscall.international/en/.

1. US Strategic Direction

The definition of critical infrastructure first appeared in the United States, and critical infrastructure was defined as a major national public project.[24] In the mid-1990s, in view of the growing threat of international terrorism, policy makers redefined it from the perspective of US homeland security.[25] Federal government reports, laws, and administrative orders have continuously expanded the number of critical basic departments and types of assets, and defined the word "critical" for homeland security purposes.[26]

In the United States, most of the critical infrastructure is operated and owned by private enterprises. The government must cooperate with enterprises to effectively protect the information security of critical infrastructure. Therefore, the law stipulates the obligation of cooperation and information sharing between the government and private enterprises to maintain network security more effectively. Internationally, information security and legal protection have been promoted as a new worldwide issue. The United States actively cooperates with other countries to formulate international laws and regulations. For example, in June 2012, Europe, the United States and Japan jointly issued Recommended Government Approaches to Cybersecurity.[27] Attaching importance to domestic and international cooperation, and effectively using even leading international rules in this field have become the development trend of the United States to ensure critical information infrastructure[28]. However, the international cooperation on critical information infrastructure advocated by the United States is a US-led cooperation, as is stated in the 2018 National Cyber Strategy.[29]

[24] *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets* (Feb. 2003), https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

[25] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56 (2001); Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, 39 WEEKLY COMP. PRES. DOC. 1816 (Dec. 17, 2003).

[26] Exec. Order No. 13,636, 3 C.F.R. 217 (2013) (Improving Critical Infrastructure Cybersecurity).

[27] Info. Tech. Indus. Council, *Global Information and Communications Technology (ICT) Industry Statement: Recommended Government Approaches to Cybersecurity* (2012), https://www.itic.org/dotAsset/69ec38f0-e17b-44df-9ac3-6fa9052c743c.pdf.

[28] Wang Kangqing, Zhang Shaowu, *Analysis and Development Trend of U.S. Critical Infrastructure Protection Legislation and Policies,* 9 Netinfo Security 45 (2015).

[29] U.S. DEPT. OF DEFENSE, SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY (2018). The document argues that in peacetime, we are vulnerable to cyber attacks on critical infrastructure. *Id.* at 1. Attackers are constantly developing new and more effective cyber weapons. Therefore, the United States should focus on strengthening network capabilities and establishing strategic partnerships. *Id.*

2. *Russia Strategic Direction*

Russia believes that the boundless nature of cyberspace determines that it is impossible for any country to solve all problems in cyberspace by itself.[30] Therefore, Russia has always advocated strengthening international cooperation in the field of cyberspace governance, and regards it as an effective means to restore Russia's status as a great power and enhance its voice in the international community.[31] In the field of international cooperation in combating cybercrime, Russia has also shown a willingness to actively cooperate.

In 2011, Russia, China, and other Shanghai Cooperation Organization countries jointly proposed the International Code of Conduct for Information Security to the United Nations, which stated that each country has the responsibility and right to protect their information space and critical infrastructure from threats, interference and attacks.[32] In October 2017, Russian leaders participated in the BRICS summit, where they reached consensus on cyber security and anti-terrorism issues, and signed cooperation agreements with China based on the consensus.[33] At the same time, Russia's Group IB company, which specializes in the prevention and investigation of cyber crime, provided Interpol with information about the "Bad Rabbit" of the encryption blackmail virus, aiming to help identify the specific perpetrators of the cyber attack.[34]

[30] On October 26, 2017, Russian President Vladimir Putin stressed strengthening regional and international cooperation in cybersecurity at the working conference of the Federal Security Council. *Putin: Cyber security is of strategic significance,* XINHUANET (Oct. 27, 2017), http://www.xinhuanet.com/2017-10/27/c_1121865749.htm.

[31] In June 2013, Russia and the United States signed a bilateral agreement on confidence building measures in the field of networking at the G8 summit in Northern Ireland. Ellen Nakashima, *U.S. and Russia sign pact to create communication link on cyber security*, WASH. POST, June 17, 2013, https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html.

[32] Annex to the letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc A/66/359 (Sept. 14, 2011).

[33] 2017-2020 Implementation Guideline for the China-Russia Treaty Between the People's Republic of China and the Russian Federation on Good-neighborliness.

In the same year, Russian President Vladimir Putin published an article leading up to the BRICS Summit in China. Vladimir Putin, *BRICS: Towards New Horizons of Strategic Partnership*, TIMES OF INDIA (Aug. 31, 2017, 9:44 PM), https://timesofindia.indiatimes.com/blogs/toi-edit-page/brics-towards-new-horizons-of-strategic-partnership/.

[34] Xianju You, *Thoughts and Practices of Russia's Information Space Construction*, 5 RUSS. E. EUR. & CENTR. ASIA STUD. 51 (2017).

3. *China Strategic Direction*

China strategically attaches great importance to the establishment of a critical information infrastructure protection system. The data[35] shows that transnational network attacks are increasingly frequent, among which APT attacks and back door attacks against domestic critical infrastructure are on the rise year by year. In addition to strengthening scientific research and preventing cyber attacks technically, China is also constantly improving its laws against cyber attacks.[36]

In view of the crimes committed by the critical information infrastructure, China advocates the provision of reasonable counter-measures. It is not only through the settlement of disputes by force that the security of national critical infrastructure can be maintained. China's newly formulated Cybersecurity Law (CSL) includes a related system designed to protect CII.[37] In 2017, China pointed out in the International Strategy of Cooperation on Cyberspace that there are great risks in key information infrastructure.[38] It also advocates jointly promoting the construction of global information infrastructure, strengthening international cooperation, and promoting countries to reach consensus on the protection of critical information infrastructure.[39]

On September 8, 2020, China also put forward the Global Initiative on Data Security, advocating that all countries oppose the use of information technology to destroy the critical infrastructure of other countries or steal

[35] The Data comes from the "China Internet Cyber Security Report" issued by the National Internet Emergency Response Center (CNCERT) during 2014–2019. Nat'l Internet Emergency Response Ctr., 2019 China Internet Cyber Security Report (2020).

[36] Jinrui Liu, *Basic Thinking and Institutional Construction of Legislation on Critical Internet Infrastructure in China*, 38 GLOB. LEGAL REV. 116 (2016).

[37] Rogier Creemers, Paulo Triolo & Graham Webster, *Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]*, NEW AM. (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Article 33 of the *Cybersecurity Law* clearly stipulates the three synchronization systems of CII, and puts forward that "[t]hose constructing critical information infrastructure shall ensure that it has the capability to support business stability and sustained operations, and ensure the synchronous planning, synchronous establishment, and synchronous application of security technical measures." *Id.* art. 33.

[38] *International Strategy of Cooperation on Cyberspace*, MINISTRY FOREIGN AFFS. PEOPLE'S REPUBLIC CHINA, at ch. I (Mar. 1, 2017), https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml.

[39] *Id.* ch. IV, art. 8.

important data, and use it to engage in acts that endanger the national security and public interests of other countries.[40]

V. STRENGTHEN THE INTERNATIONAL COOPERATION FOR CII PROTECTION

1. Strengthen International Judicial Cooperation

International cooperation in combating critical information infrastructure crimes, or joint implementation of critical infrastructure protection mainly relies on the domestic jurisdiction of each country. Therefore, strengthening the protection of critical infrastructure requires strengthening judicial exchanges and cooperation between countries and regions. To strengthen legal coordination and judicial cooperation, we need to reach a consensus on common threats and cooperation outlines. By studying, comparing and sorting out the relevant domestic laws of the partners, we seek compromise and consensus on the judicial aspects of the contradictions, so as to jointly formulate the legal basis for bilateral and regional cooperation. In addition, we should strengthen police cooperation and judicial assistance, and sign cooperation agreements with law enforcement departments. In particular, it is necessary to study the ways of cooperation between relevant countries in the event of an emergency.[41]

Second, strengthen international exercises to deal with information risks of critical information infrastructure. Through joint network exercises, weak links in the field of information security assurance can be identified, and the countermeasures for these issues can be incorporated into the legislation for the security assurance of critical information infrastructure.

[40] *Global Initiative on Data Security*, MINISTRY FOREIGN AFFS. PEOPLE'S REPUBLIC CHINA, (Sept. 8, 2020), https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml.

[41] Zeliang Zhao, *The New Connotation of Improving the Information Security System under the New Situation*, 12 CHINA INFO. SEC. 93 (2013).

2. *Strengthen International Cooperation in Network Vulnerability Management*

Vulnerabilities exposed on the Internet are one of the main reasons behind most network intrusions[42]. With the development of the Internet of Things, the potential impact of vulnerability attacks on critical information infrastructure is increasing.

On November 12, 2018, the 100th anniversary of the signing of the Armistice Agreement of the First World War, French President Macron delivered a speech during the 13th United Nations Internet Governance Forum (IGF), proposing the Paris Call for Trust and Security in Cyberspace ("Paris Call").[43] The Paris Call also talked about the issue of vulnerability governance, stating that "all actors can support a peaceful cyberspace by encouraging responsible and coordinated disclosure of vulnerabilities."[44] At least 79 countries, 688 private companies, and 374 related organizations have signed the Paris Call, and the number of supporters may continue to increase.[45]

Based on the impact that the Paris initiative has had on the international community, international cooperation on the governance of loopholes in cyberspace has already developed a basis of support.[46] We can promote international consensus with academic strength by holding a symposium on cyberspace and an international seminar on cooperation in vulnerability management. Through the initiative and promotion of relevant government agencies on the international stage, the effective cooperation between all parties will be gradually realized.

[42] Meneghello F, Calore M, Zucchetto D, et al. *IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices*, 6 IEEE INTERNET OF THINGS JOURNAL 8182-8201 (2019).

[43] Emmanuel Macron, 2018 Internet Governance Forum Speech (Nov. 12, 2018), https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron.

[44] Paris Call for Trust and Security in Cyberspace, Nov. 12, 2018, https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

[45] *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace,* MINISTRY EUR. & FOREIGN AFFS. (Feb. 2012), https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[46] At present, more than 74 countries, 350 international, civil society and public sector organizations, and 600 private sector entities have signed the Paris Cyberspace Trust and Security Initiative, and expressed concern and support for cooperation in maintaining the order of cyberspace. John Frank, *Paris Call: Growing Consensus on Cyberspace,* MICROSOFT ON THE ISSUES (Nov. 12, 2019), https://blogs.microsoft.com/on-the-issues/2019/11/12/paris-call-consensus-cyberspace/.

3. *Set Up a Unified Coordination Agency for International Cooperation*

To carry out international cooperation to combat critical infrastructure crimes, we must first establish an international coordination organization to work on the basis of peace and democracy. Cyber attacks against critical infrastructures should first be resolved peacefully through peacetime laws, by following the principle of peaceful coexistence to strengthen cooperation and exchanges between countries on this issue.[47]

Second, determine the legal status of the United Nations in resolving related disputes and coordinating the interests of all parties. In response to the high incidence of cyber crime and the proliferation of cyber terrorism, the international community has begun to adopt active prevention strategies. In this context, it is even more important to promote the role of the United Nations. It has been agreed that one or more comprehensive legal instruments designed to prevent threats to critical information infrastructure have been formulated through the United Nations.[48] In recent years, the United Nations has made efforts to ensure cybersecurity through legislation. For example, in 1994, the United Nations issued the United Nations Manual on the Prevention and Control of Computer-Related Crime.[49] In June 2016, the SCO adopted the Tashkent Declaration, which declared that member states support the formulation of universal norms, principles, and guidelines for responsible state behavior in cyberspace within the framework of the United Nations.[50]

Third, set up a special international cooperation organization to ensure network security and critical information infrastructure. There are already a

[47] Annex to Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, art. 12, U.N. Doc. A/69/723 (2015) (advocating that any disputes shall be resolved peacefully, and no force or threat of force shall be used).

[48] In June 2013, Deputy Secretary-General of the United Nations, Peter Lonski Tiffenso gave an interview with the Chinese news agency Xinhuanet, which reported that Tiffenso "believes that cyber" security is one of the challenges that need to be solved collectively, and the United Nations is a platform for responding to global challenges. Therefore, cyber security issues as a global challenge need to be solved by the United nations. *United Nations: Cybersecurity Is a Global Challenge to Be Solved by the United Nations*, XINHUANET (June 27, 2013, 8:22 PM), https://world.huanqiu.com/article/9CaKrnJB4VM.

[49] U.N. Ctr. for Soc'y Dev. & Humanitarian Affs., International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-Related Crime, U.N. Doc. ST/ESA/SER.M/43-44, U.N. Sales No. E.94.IV.5 (1994).

[50] The Tashkent Declaration of the Fifteenth Anniversary of the Shanghai Cooperation Organization, EMBASSY REPUBLIC UZB. IN REPUBLIC LAT. (June 28, 2016), http://uzbekistan.lv/en/the-tashkent-declaration-of-the-fifteenth-anniversary-of-the-shanghai-cooperation-organization/.

large number of international cooperation institutions to ensure network security, including but not limited to The United Nations Educational, Scientific and Cultural Organization,, International Telecommunication Union and Internet Content Rating Association. However, the general limitation of these organizations is that they often advocate technical control in their adjustment methods, with industry and user self-discipline as the main means. This is very different from the way the government regulates the Internet. Therefore, it is necessary to set up a special international organization to ensure the security of critical information infrastructure. For example, the INTERPOL Global Complex for Innovation (IGCI), established by INTERPOL in 2014,[51] provides a platform for cooperation between national governments, international organizations, regional policing bodies and the private sectors.[52] At this stage, the IGCI can be used as a professional cooperation platform to attract more countries to participate, give it an international legal status to protect network security and critical information infrastructure, and expand its scope of functions. The rights of the organization in the investigation, arrest, and acquisition of evidence should be clarified in the form of law.

[51] *INTERPOL Global Complex for Innovation Opens Its Doors*, INTERPOL (Sept. 30, 2014), https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors.

[52] It includes police officers from government organizations and technical experts from private organizations. The list of specific cooperative organizations can be found on the official website. *What is INTERPOL?,* INTERPOL, https://www.interpol.int/Who-we-are/What-is-INTERPOL (last visited June 12, 2021).

VI. CONCLUSION

In terms of legislation on critical information infrastructure, countries have formed different legislative systems for critical information infrastructure protection based on their own technological level and social governance status. However, due to the complexity of the protection of critical information infrastructure, even major countries such as China, the United States and Russia are still in the process of solving problems. For the protection of critical information infrastructure, countries need to actively seek common experience in the process of existing policies and legislative practices, exchanges and cooperation with other countries, and build a global cyberspace community with a shared future. In the course of practice, it should be characterized and punished according to the law in peacetime. Finally, countries should try to strengthen international cooperation in cybercrime through an agreement from bilateral cooperation to multilateral cooperation.