

The Governance Mechanism and Process of Global Cyberspace Security Under the Framework of the United Nations

Zhi Li ¹, Tang Zheng ², Yuemeng Ge ², Jia Min¹, Danqi Chen ^{1*}

¹ School of Media and Law, NingboTech University, Ningbo, China;

² School of Business, Zhejiang Fashion Institute of Technology, Ningbo, China

* Corresponding author: lizhi@nit.zju.edu.cn

Abstract: Since the security of global cyberspace was regarded as the core topic of global governance, the UN has become the main place for exchanging ideas, developing debates and promoting governance. Therefore, the global cyberspace governance mechanism established by the United Nations is naturally acclaimed as the most representative platform, providing opportunities and assistance for the countries all over the world to participating in the global cyberspace governance. For the governance mechanism and process of global cyberspace security, the UN has not only set global agendas on the right to free speech on the Internet, the sustainable development of cyberspace security, the inclusiveness of the artificial intelligence and the sustainable development, but also has established a relatively integrated the framework of the governance mechanism. In dealing with the differences and games in the changing of the global cyberspace security governance, the UN still condenses consensus and continuously promotes the international cooperation, pushing the security of global cyberspace become the general consensus in the international community. Meanwhile, the UN also calls for countries around the world to coordinate governance in order to consolidate and develop the status of the United Nations in global cyberspace security governance.

Key words: The United Nations, Framework, Cyberspace Security, Governance Mechanism, Process

Tob Regul Sci.™ 2021;7(5-1): 3685-3697

DOI: doi.org/10.18001/TRS.7.5.1.145

1. Introduction

The cyberspace, whose form extends and differentiates from the social space with the development of the network technology, is another important living space for people in the Internet age. The new definition of the cyberspace is based on the framework of communication technology infrastructure, network data information, and ICT application activities which carried by human being. In addition, cyberspace supports the construction of highly integrated and interactive artificial spaces with other spaces, reflecting the uniqueness of cyberspace governance and the social value of cyberspace [1]. Global cyberspace security is the key to studying about information security in the field of information acquisition, storage, transmission and processing. It is formed by the integration of computer, electronics, telecommunications, mathematics, physics, communications, management, law and education. It both has its own connotation, theory, technology and application, but also serves cyberspace. The global cyberspace governance has become the primary task of global governance. Because it is about the overall situation of every country's security, economic and social development, as well as the national interests and people's fundamental interests. As an advocate of world norms, the UN plays a particularly prominent role in the governance mechanism and process of global cyberspace security. Normally advocates of norms are politicians, diplomats, military personal and academics. The essence of it is that anyone

who owns enough resources can make a difference and become a norm advocate. There is no doubt that the UN and the role are very matchable. The reason is that the United Nations officials themselves are advocate of norms, which produces international laws and norms as a result of diplomatic activities [2].

2. Agendas Related to Global Cyberspace Security Under the Framework of the United Nations

The high degree of integration between Internet technology and people's lives in the world has also brought some problems in real life, and has even evolved into cyberspace security agendas of general concern at the national level.

Firstly, it is the issue of the right to free speech on the Internet. As early as 2012, the United Nations Human Rights Council carried a wide range of discussions on the right to free speech at the Internet, pointing out that the right to freedom of speech on the Internet is currently facing a main issue. Meanwhile, the UN also clearly identified that member states can take practical measures to protect their freedom of speech on the Internet. The United Nations Human Rights Council believes that the main issues need to focus on the protection of Internet freedom of speech are: 1) face up to the role of the Internet in protecting human rights; (2) attach importance to the possibility of committing crimes by using the Internet. Internet activities are now showing a trend of criminalization, such as

endangering national security and social stability, inciting hatred, making falsehoods, child pornography, and trafficking in persons, etc. (3) Freedom of speech on the Internet should be formulated in compliance with international laws and related standards in order to face a large number of surveillance software are used to violate personal privacy rights; (4) Call for cooperation and sharing of network technology to reduce the digital divide between countries around the world; (5) Clear the connotation of intellectual property up. The solution to the issue mainly focuses on relevant international norms and standards, determining the application of international human rights law, ensuring the free flow of Internet information, and reiterating the strengthening of the implementation of the current principles of international human rights law on the Internet. The Human Rights Council discussed the right to freedom of expression on the Internet respectively at the 20th Conference on Racism, the 23rd Conference on Freedom of Speech, the 28th Conference on Child Crime, and the 29th Conference on the Promotion and Protection of Human Rights [3].

Secondly, it is the issue of the sustainable development of cyberspace security. In order to promote the sustainable development of global cyberspace security, the United Nations has had great concern for the issue of the improvement of infrastructure and the reduction of the digital divide in the field of global cyberspace governance. For example, the UN 2030 Agenda

for Sustainable Development, one of the goals of which is to promote innovative development, improve infrastructure construction, and reiterate the accessibility of the internet expansion is a necessary measure for the successful implementation of this agenda. Simultaneously, the agenda also proposes to "Significantly increase the popularity of information and communication technology, and strive to provide Internet services for the least developed countries at low prices by 2020" [4]. In some ways, that means significantly expanding the audience's access to network security information and communication technology. In addition, the topic of the UN 11th Internet Governance Forum (IGF) is promoting Inclusive and sustainable growth, in which mainly focuses on discussing the future of the worldwide Internet, including how to utilize the Internet to better promote the inclusive and sustainable development of the world and ensure that the bonus brought by global cyberspace security can be shared with developed and developing countries.

Thirdly, it is the issue of the inclusive of artificial intelligence and sustainable development.

The main platform of the United Nations Artificial Intelligence Dialogue is the AI for Good Global Summit, which is a specialized agency of the United Nations Information and Communication Technology. This annual summit is jointly organized by the International Telecommunication Union (ITU) and various branches of the United

Nations. Its purpose is to consolidate world's consensus on the improvement of emerging artificial intelligence technology abilities. For example, at the first summit held in Geneva in 2017, a global dialogue on the benefits of artificial intelligence was launched. At the second summit in 2018, a strategic development and support project with artificial intelligence was formulated to promote the rapid realization of the UN's sustainable development goal, and to jointly formulate a global strategy with multiple stakeholders. These will ensure the safe, reliable and inclusive development of AI technology. Especially during the 2018 summit, ITU and the United Nations Department of Economic and Social Affairs, UNEDA, UNESCO, UNHCR, WHO, Intellectual Property Organization and the World Bank Group, a total of 32 institutions, held the second UN Partners Meeting on May 16. In this meeting, they further discussed the role of various agencies in the sustainable development and governance of artificial intelligence, and strived to strengthen the partnership between various UN agencies, expand the innovative solutions based on artificial intelligence, and promote sustainable development.

3. The Construction of the UN Security Governance Mechanism in Global Cyberspace

The core of the United Nations is the Charter of the United Nations, which provides the legal framework for different actors of the United Nations and has become the most accurate

expression of the conceptualized relationships. The United Nations actors are composed of three parts: the first part is the Security Council, which consists of 15 member states; the second part is the Economic and Social Council (ECOSOC), with 54 member states participating in; the third part is the General Assembly, which is composed of 192 member states. Diplomats are actors of United Nations acting subjects. And the United Nations Secretariat is the decision-making body of actors, which is led by the Secretary-General of the United Nations. The United Nations actors are subordinate agencies. According to Article 22 of the UN Charter, they can be both an auxiliary agency and also be a specialized agency in accordance with Article 57 of the Charter of the United Nations. At the same time, in accordance with Article 22 of the "United Nations Charter", member states of the United Nations agree to accept and implement the resolutions of the Security Council in accordance with the constitution. Therefore, the Security Council is the only legal body that has the power to formulate binding international laws. In addition, according to Articles 10 and 12 of the United Nations Charter, the United Nations General Assembly can only exercise the right to make suggestions. Obviously, the governance framework built by the United Nations, the "United Nations Charter," plays a very important role.

The global cyberspace security governance mechanism established by the United Nations is

the most representative force in the world, providing opportunities and assistance for countries around the world to participate in the cyberspace governance agenda. As far as the process of global cyberspace security governance is concerned, the United Nations has not only built a relatively complete mechanism system, but also has acted as an important governance platform and participant. In some ways, its power cannot be ignored. The relevant governance mechanisms established by the United Nations in the field of global cyberspace mainly include the United Nations Group of Governmental Experts on Information Security, the Government Expert Group Against Cybercrime, the World Summit on the Information Society, the Internet Governance Forum, and the International Telecommunication Union.

The United Nations has the UN Group of Governmental Experts on the issue of information security (UNGGE), which is mainly organized by the Disarmament and International Security Committee. The discussion agendas of the expert group mainly focus on the capabilities of the national network security, the application of international law, and the role of the United Nations in cyberspace security issues. They strive to "Review existing and potential threats in the network field, and take possible cooperative measures to solve these threats" [5]. Moreover, the expert group agreed for the first time in the 2013 report that international law is applicable to cyberspace governance, that is the international

law, especially the Charter of the United Nations. The principle of national sovereignty applies to countries' activities related to information and communication technology, and has the jurisdiction over the ITC infrastructure within its territory; it can also assess state behavior to reduce the risk of conflict, and help developing countries improve their capabilities of information technology [6].

The United Nations was founded to discuss and establish a platform for international rules to combat cybercrime. Each year, the conference respectively discusses issues about the criminalization of cybercrime legislation, conviction, investigation, electronic evidence, international cooperation, prevention, etc. In the previous conferences, the focus of the expert group's debate is whether it is necessary to formulate a new convention against cybercrime, or whether to continue to promote the use of the European Union Budapest Cyber-crime Convention (Cyber-crime Convention). Besides, in 2013, the United Nations Office for Drug Control and Crime Prevention (UNODC) also authorized the secretariat of the expert group to compile the Draft Comprehensive Study on Cybercrime, which mainly studies the global cybercrime trends, characteristics, hazards, current international situations and policy limitations, etc. And they also explore solutions in terms of formulating comprehensive global norms, international model clauses, and strengthening technical assistance to developing countries [7].

The main purpose of the World Summit on the Information Society (WSIS) is to formulate plans for the coordinated development of the information society on a global scale, using information technology to promote the realization of the United Nations Millennium Development Goals, promoting the sustainable economic and social development of various countries, and finally promote the overall human progress. From 2002 to 2005, WSIS respectively held two summits----the Geneva Summit and the Tunis Summit. The Geneva Summit adopted the Declaration of Principles and the Action Plan. And the Tunis Summit adopted the Tunis Commitment and the Tunis Agenda, both of which are programmatic documents. WSIS has proposed a "multi-stakeholder" model to give the private sector and civil society the legitimacy to participate in global cyberspace governance [8].

The Internet Governance Forum (IGF) is authorized by WSIS and aims to be a multi-stakeholder platform for discussing public policies in cyberspace on a global scale, and is committed to promoting policy dialogue and communication among countries. In July 2006, the Secretary-General of the United Nations announced that Internet governance forums would be held in different countries every year. The topics are mainly focused on eliminating the "digital divide", maintaining network security, protecting the diversity of network development, popularizing the Internet, and managing network resources [9]. The Internet Governance Forum has had a

positive impact on global cyberspace governance and promoted the world's consensus on global cyberspace issues, including the development of the diverse network culture, and strengthened the participation of various stakeholders in global cyberspace security governance cooperation on technical and other issues, including the capabilities of the cyberspace governance agenda. That has improved global cyberspace security and sustainable development.

The International Telecommunication Union (International Telecommunication Union, ITU) is an organization of the United Nations, which is responsible for network security incidents and assists in the management of communication protocols between countries. This is also the only organization in the United Nations that works on cyber issues as a treaty organization. ITU existed before the establishment of the United Nations. According to Article 57 of the United Nations Charter, ITU was incorporated into the United Nations system as a specialized agency. It plays an important role in setting technical standards and is managed by a large organization of technicians who have specialized areas of focus, such as smart grid infrastructure [10]. ITU calls the global space cybersecurity agenda an international framework for cybersecurity [11]. The Global Cyberspace Security Agenda proposes legislative models that can be adopted by ITU member states, and assists member states to use the Budapest Cybercrime Convention as a legislative example. After 2000, the ITU's focus has shifted from information and

communication technology to the Internet, striving to play a role in global cyberspace governance and make it the foundation of the global cyberspace security governance system.

4. The Process of the United Nations Security Governance Mechanism in Global Cyberspace

It has become a general consensus to promote international multilateral cooperation and jointly govern global cyberspace security under the framework of the United Nations. As the representative of the multilateral platform, the United Nations is the main place for member States to exchange ideas, debate and further promote the governance mechanism on the issues of global cyberspace security governance. It also carries the main process of international law on global cyberspace security. These processes are as follows:

First, some differences in the multilateral process have been blocked and moved forward, mainly reflected in the "dual-track" system of UNGGE and the Open-ended Working Group (OEWG). In terms of participation, UNGGE is closed, which ensures that the expert group can fully express its views to a certain extent, but it also faces various speculations caused by the lack of transparency. UNOEWG is open and open to all members of the United Nations, with the characteristics of being more extensive, more democratic, more transparent, more pluralistic and more inclusive. In terms of governance efficiency, UNGGE sets the number of participants, making

it more in-depth, more specific and easier to reach consensus on issues. UNOEWG has a wider range of participation, but the differences are also very prominent, not only between countries, but also from different stakeholders. The reports reached by UNGGE in 2013 and 2015 build the basic consensus of the international community on the code of conduct for global cyberspace security, and are recognized as an important place for negotiations on global cyberspace security governance mechanisms [12]. Since the UNGGE fell into disagreement in 2017, the prospect of multilateral negotiations on the United Nations global cyberspace security governance mechanism has also been seriously hindered. Later, the sixth UNGGE and the OEWG were respectively established and carried out relevant work, which marked the completion of the restart of the United Nations global cyberspace security governance mechanism, and its effect is worthy of affirmation. For example, when the OEWG held its first meeting in September 2019, most member states pledged to accept the 11 norms mentioned in the 2015 UNGGE report, and agreed that feasible measures to promote responsible State behavior in global cyberspace would be discussed next.

Second, some multilateral processes have advanced consensus building in an orderly manner, which is mainly reflected in arms control negotiations on lethal autonomous weapons systems. Since the establishment of the Group of Governmental experts on emerging Technologies

in the Field of lethal Autonomous weapon Systems in the United Nations Convention on conventional weapons (CCW Convention) in 2017, (LAWSGGE) has continued to advance relevant work in accordance with the established plan. LAWSGGE held two meetings in 2019, and the topic process was mainly carried out from the technical, ethical, legal, military and other aspects related to LAWS [13]. After several rounds of negotiations, "At the technical level, the member states basically agree that LAWS arms control should not hinder the innovation of civil ARTIFICIAL intelligence technology, and there were differences on whether and how to formulate the feasible definition of LAWS and other issues at present; At the ethical level, the member states basically believe that the decision of life and death should not be transferred to machines, and there are differences on whether machines should be regarded as moral subjects. At the legal level, the member states basically agree that the existing international humanitarian law is still applicable to the control of LAWS, and have differences on whether it is necessary to increase the supervision mechanism in addition to the existing international law; At the military level, the member states basically agree that the responsibility for developing and deploying the LAWS lies with countries and commanders, and there are differences on such issues as preventive prohibition or temporary laissez-faire, or even encouraging the development of LAWS" [14]. At present, there is a substantial consensus on several

key issues of LAWS, although it is still impossible to predict when the withdrawal will be reached, the mechanism of advancing the negotiation process in the existing United Nations multilateral treaties shows that a feasible scheme of international governance can be gradually reached through consultation on the issue of global cyberspace security.

Third, there are fierce and continuous progress in the multilateral process game, which is mainly reflected in the field of international cooperation in cracking down on global cybercrime. The European Union and the United States mainly focus on the Budapest Convention to find the practice of governance mechanism and the breakthrough point of expanding governance paradigm. Through the Convention Committee's attempt to track, evaluate and improve the effectiveness of implementation, and continue to advance negotiations under Additional Protocol II on cross-border electronic forensics, to promote the accession of new States parties to strive to achieve the expansion of the treaty system. Under the multilateral framework of the United Nations, Russia and China respectively continue to formulate multilateral rules on combating global cybercrime. Russia submitted the United Nations Convention on Cooperation in Combating Information Crimes (DRAFT) to the United Nations, which was adopted by the Third Committee of the General Assembly in November 2019. However, the DRAFT caused unease and opposition from the United States and the

European Union. In spite of this, Russia has launched a mechanism worth tracking: the process of formulating multilateral treaties on global cybercrime. In addition to cooperating with and supporting the Russian program, China has also continued to promote the compilation of the United Nations Governmental Expert Group mechanism on Cyber Crimes, and at the fifth expert group meeting held in March 2019, it was agreed to accept the guidance of the international legal framework under the framework of the United Nations to combat cybercrime and build a reasonable regulatory mechanism for procedural issues of international cooperation, including cross-border electronic forensics. It can be seen that the path game created by the European Union and the United States with Russia and China on the international mechanism for combating cybercrimes has constituted a new field worthy of continuous attention in the international law of global cyberspace.

5. The challenges in promoting global cyberspace security governance within the framework of the United Nations

Global cyberspace security issues need to be addressed hand in hand by all countries. And the United Nations which as the platform to meet global challenges should be the driving force in addressing them. In view of the particularities of global cyberspace and the sensitivity of security in cyberspace, particularly countries' different perceptions of code of conduct and resource allocation of the nature of global cyberspace, the

nature of network power and multi stakeholder actors in global cyberspace. The differences in the current global cyberspace security governance mechanism, governance process and governance path are becoming more and more evident. Since 2013, although the United Nations has taken positive measures to promote the governance process of global cyberspace, the ability of the United Nations to play a leading role in global Cyberspace Security Governance is difficult. The challenges are:

(1) There are many difficulties in the technical supervision of global Cyberspace Security. In terms of technology, international negotiations on global Cyberspace Security lack a common language and foundation, and some key terms have not yet formed a unified definition that makes it difficult to track and respond to network attack. So it is very difficult to define the source of network attack.

(2) The governance objects of global cyberspace security are diverse and complex. Global cyberspace governance covers a wide range of areas. It not only includes the actors of various stakeholders, but also integrates all the different stakeholders into the framework of cyberspace governance. It can be concluded that the objects of network governance come from different groups and are diverse and complex.

(3) The information cooperation and sharing of global cyberspace security is limited. The governance of global cyberspace security issues requires the use of cutting-edge information

technology. However, most of the United Nations Member States' research and technology in this field belongs to the state of confidentiality and blockade. The information technology cooperation and technology sharing between them are very limited. As a result, the global Cyberspace Security can't be shared in time, so that the governance of global Cyberspace Security is very passive.

(4) The development of global Cyberspace Security has not been paid enough attention by Internet underdeveloped countries. The security of global cyberspace is very important and urgent for the big countries with obvious international politics and economy and developed Internet. However, for many countries with relatively backward network information technology and underdeveloped Internet, the development of Cyberspace Security is far less important than national economic development. Even the governments have not formed a unified consensus. Fortunately, after the Snowden incident, the Internet underdeveloped countries have paid attention to the global cyberspace security.

Of course, the trend of promoting global cyberspace security governance under the UN framework is also very obvious. Global cyberspace security is the core content and 'invisible' barrier of national security. The application of Internet technology is developing rapidly. This also makes the vulnerability and unbalanced development of cyberspace increasingly prominent. The 'prism gate' incident

particularly marks that all countries in the world begin to face up to their own Cyberspace Security. Even its status has gone beyond the scope of national security and evolved into a challenge that the international community should jointly cope with. International cooperation in global Cyberspace Security and playing a leading role under the framework of the United Nations is the future development trend.

There is no doubt that the United Nations is the most legitimate and authoritative international organizer in the current international relations. Relevant issues of global importance have made progress through negotiations under the framework of the United Nations, and have become the best platform for global cyberspace security governance. As mentioned above, the United Nations and its subordinate governance mechanisms have played an important guiding role in the early governance cooperation of global cyberspace security. For example, the International Telecommunication Union (ITU), a subsidiary of the United Nations, has been actively engaged in combating global cybercrime in the field of telecommunication infrastructure cooperation. In addition, the United Nations has shown a positive attitude towards the international governance of global cyberspace security. In 2013, under Secretary General of the United Nations, Peter Laursky, said that 'global cyberspace is one of the challenges that need to be solved by all of us, and the United Nations is a platform to deal with global challenges. As a global challenge,

cyberspace security issues need to be solved by the United Nations' [15].

At present, under the framework of the United Nations, global cyberspace security governance has also made some progress. Since the United Nations Expert Group (GGE) submitted the 'report on the application of the existing joint charter to cyberspace' to the general assembly in June 2013, it has been widely recognized by the international community and has become a driving force for the development of global cyberspace security governance mechanism and process [16]. At the same time, <Comprehensive research report on cybercrime> prepared by the Secretariat of the United Nations expert group is considered by most member states to be a comprehensive multilateral legal instrument and model clause for international cooperation in combating cybercrime, which is widely representative in the practice of the process. In addition, multi stakeholder actors, such as the European Union, ASEAN, SCO and other international organizations, emerging countries such as China, Russia, India, Brazil and some developing countries have made it clear that under the framework of the United Nations, it is necessary to give full play to the leading position and role of the United Nations in global Cyberspace Security Governance, and promote the governance process of cyberspace forward.

Therefore, in the face of the complexity and internationalization of global cyberspace security issues, any single multi stakeholder is unable to

deal with the increasing network threats and challenges. Under the framework of the United Nations, it has become a common consensus of the international community to promote international bilateral and multilateral cooperation and jointly govern global cyberspace security issues. It has promoted the position of the United Nations in global cyberspace governance to be further consolidated and developed.

6. Conclusion

Issues related to global cyberspace security under the framework of the United Nations cover the right to freedom of speech on the Internet, the sustainable development of cyberspace security, the inclusiveness and sustainable development of artificial intelligence. In the process of constructing the global cyberspace governance mechanism, the Charter of the United Nations is the foundation of the legal framework. The United Nations Information Security Government Expert Group, the Government Expert Group Against Cybercrime, the World Summit on the Information Society, the Internet Governance Forum and the International Telecommunication Union have become global the most representative cyberspace security governance mechanism provides opportunities and assistance for the participation of member states. Although the governance mechanism of the United Nations in global cyberspace presents a multilateral process, it still builds consensus, moves forward and continues to advance in the face of blocked differences and fierce competition. Undoubtedly, the United

Nations, as an important participant and platform in global cyberspace security governance, is still confronted with difficulties in global cyberspace technology supervision, diverse and complex objects of cyberspace governance, limited cooperation and sharing of network information, and insufficient attention of underdeveloped countries in developing the internet. However, it is undeniable that under the promotion of the United Nations, international bilateral and multilateral cooperation and joint governance of global cyberspace security have become the universal consensus of the international community, and its role should not be overlooked.

Acknowledgments

This work was supported by the National Social Science Fund of China of the Youth Project “A Comparative Study on the Laws of Global Cyberspace Security Governance and Its Enlightenment to China” (Grant No. 19CXW039).

References

1. Li Zhi. (2020), The Cyberspace of Conception, Exchange and New Definition. China Media Report, 19(02): 12.
2. Tim Maurer, Qu Tian and Wang Yan. (2017), The emergence of United Nations network norms: an analysis of UN cyber security activities, Journal of Shangtou University (Humanities and Social Science), 33(5): 4-105.
3. United Nations Human Rights Council. (2016), <https://www.ohchr.org/EN/HRBodies/HRC/Pages/Home.aspx>.
4. Ministry of Foreign Affairs of the People's Republic of China. (2016), Transforming our World: The 2030 Agenda for Sustainable Development. https://www.fmprc.gov.cn/web/ziliao_674904/zt_674979/dnzt_674981/qtzt/2030kcxzfzyc_686343/t1331382.shtml.
5. United Nations Office for Disarmament Affairs. (2013), Fact Sheet-Developments in the Field of Information and Telecommunications in the Context of International Security. http://unoda/eb.s3.amazonaws.com/acontent/uploads/2013/06/Information_Security_fact_Sheet.pdf.
6. Adam Segal. (2016), The UN's Group of Governmental Experts on Cybersecurity. <https://www.cfr.org/blog/uns-group-governmental-experts-cybersecurity>.
7. Wang Tianchan. (2019), The United Nations and the process of cyberspace national law. Information Security and Communication Privacy, (05): 7-9.
8. Wang Mingguo. (2015), Model change, institutional logic and Reconstruction Path of global network governance. World Economics and Politics, (03): 86.
9. What is the Internet Governance Forum? (2018), <https://www.intgovforum.org/multilingual/chinese/content/about-igf-faqs>.
10. United Nations International Telecommunication Union. (2008), "ITU Global Cybersecurity Agenda: High Level Experts Group— Global Strategic Report", Geneva: United Nations, 95.
11. Yu Jianhua, Liu Jinqian. (2020), The Latest Security Situation and Future Development of “The Current Kashmir Dispute” between India and Pakistan. Studies on Foreign Social Sciences, 43.
12. Yang Fan. (2020), New developments and new trends of

international law in Cyberspace. Information Security and Communication Privacy, (01): 30.

13. Xu Nengwu, Long Kun. (2019), The Focus and Trend of Debate on Arms Control of Lethal Autonomous Weapons Systems under the UN CCW Framework. Journal of International Security Studies, (05): 1.
14. UN: cyber security is a global challenge to be solved by UN. (2013), Xinhua Net. <https://world.huanqiu.com/article/9CaKrnJB4VM>.
15. UNODA. (2013), Developments in the Field of Information and Tele-communications in the Context of International Security. http://www.un.org/disarmament/HonlePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.
16. Lu Chanying. (2013), On the dilemma of global governance in Cyberspace, Contemporary International Relation, (11): 31.