The Past, Conundrums, and Future of International Cybersecurity Governance

Guan Yongping

Guangdong University of Finance & Economics, Guangzhou, 510320, Guangdong, China

Abstract: *Due to the growing reliance of nations on the Internet, cyber security concerns have become a global concern for the entire international community. After the international community has acquired a consensus on the principles of international cyberspace governance, it stalls due to the delay in obtaining an agreement on the application of international law. The governance of global cyberspace security is currently confronted with challenges such as nations' divergent interests and values and the expansion of international competition into cyberspace. In the future process of establishing an international order in cyberspace, the "dual-track system" of the United Nations should be utilized in its entirety, national collaboration at the regional level should be encouraged, and the legislative road of "multilateralism" should be adhered to.*

Keywords: *Cyberspace Security, International Governance, Multilateralism*

Cyberspace is currently the "fifth space" of human life, after land, sea, air, and outer space, and it presents both opportunities and difficulties.[1] Because of the growing reliance of nations on the Internet, cyber security concerns have become a global concern for the entire international community. There is no country that could stand alone against cyber security threats as cyberspace is interactive and open in nature and the deepening convergence of the interests of all countries in cyberspace. A secure, stable, and harmonious cyberspace is vital to the international community.

1. The development of the international rule of law's expansion into cyberspace

Since the birth of the Internet, the prevailing opinion regarding the administration of cyberspace has been that it was an "autonomous system" that could self-regulate without the intervention of real-world governments. However, as the Internet has gradually become integrated into all facets of human society and as various forms of online misconduct and security threats have become apparent, the international community has begun to recognize the significance of cyberspace governance and the fact that it could no longer develop unchecked.

1.1. Cyberspace security gained an international perspective.

On 4 January 1999, the United Nations General Assembly enacted resolution A/RES/53/70, requested by the Russian Federation, which for the first time, addressed information and telecommunications challenges within the context of international security.[2] In 2002, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications was founded. Therefore, cyberspace security was added to the official international agenda.

1.2. International consensus reached on cyberspace governance.

The 2007 attack on the Estonian network and the 2010 Stuxnet virus strike on Iran indicated that when cyber operations were explicitly directed and targeted, their reach and impact could be expanded, posing a greater security risk. Simultaneously, both occurrences were political, and although the countries involved denied involvement, occurrences demonstrated that they could use force by launching cyber strikes.[3] Therefore, countries had begun adopting cyber security plans and actively participating in international conferences on cyber security rule-making to create consensus on international governance in cyberspace, such as the 2011 US Strategy for Operating in Cyberspace.

At the 68th session of the United Nations General Assembly in 2013, the Third Panel of Experts presented a "landmark" consensus report. The report emphasized that cyberspace was an international arena and that the behaviour of states in cyberspace was constrained by current international law, specifically the UN Charter. This consensus report, for the first time, acknowledged the relevance of international law to establishing order in cyberspace, signifying that the international community had formed a consensus on the global governance of cyberspace based on shared principles.

1.3. International cyberspace security governance was at a standstill.

While the international community had developed a consensus on the applicability of international law in cyberspace, governments held different perspectives on how existing international law, especially its principles and articles, could apply in cyberspace. In the draft report submitted by the 5th Group of Governmental Experts (2016-2017), reference was made to the application of the right to self-defence, international humanitarian law, the law of state responsibility, and the countermeasure principles of general international law in global cyberspace security governance, which the states represented by Cuba opposed.[4] The 5th UNGGE was unable to present a consensus report in 2017, and the discussion among nations over international cyberspace security governance reached a logjam.

1.4. The UN's "dual-track" platform emerges.

To break the logjam, the UN established the Open-Ended Working Group in 2018, which is open to all member states and, along with UNGGE, forms the UN's "dual-track system." The UNGGE comprises sovereign states that investigate the specific application of international law to cybersecurity challenges and support the creation of international standards applicable to cybersecurity governance, such as norms of responsible state conduct.[5] Although the core mandate of UNOEWG is identical to that of UNGGE, the establishment of UNOEWG has broadened the scope of international governance in cyberspace: developing countries have begun to participate in establishing an international security order in cyberspace. They can now express their views and opinions on cyberspace security governance on a global stage. During the first substantive session of the UNOEWG in September 2019, several countries identified cybercrime and cyberterrorism as critical security risks in cyberspace. They presented their proposals for establishing an international order in cyberspace. In 2021, the UNOEWG and the UNGGE completed their consensus reports successively.[6] From 28 February to 11 March 2022, the first negotiating session of the UN Convention against Cybercrime was held successfully, and all parties involved in the negotiations supported the formulation of the UN Convention against Cybercrime as soon as possible in light of the growing international cybercrime problem.

2. The present challenges of international cyberspace governance

2.1. State interests in international cyberspace security governance vary.

There are primarily two camps on international cyberspace security governance: the cyber technology powerhouse led by the United States, emphasizing "Internet freedom," and the vast majority of technologically impoverished developing nations, represented by China and Russia, emphasizing "protecting cyber sovereignty." These two contradictory claims reflect the divergent objectives of the two camps.

The industrialized Western nations, led by the United States, have always been at the forefront of technology, have a first-mover advantage in cyber technology, and wield a degree of influence and domination in developing international cyber security regulation. As a result, they hope to use their existing advantages to promote "Internet freedom" in the global governance of cyberspace in line with their interests and establish a cyber-order conducive to their development to facilitate access to additional cyber benefits and resources to bolster their comprehensive cyber capabilities. For instance, America, the foundation of the Internet, has repeatedly claimed that it will build cybersecurity cooperation based on "shared values and similar interests."

Developing countries, which are in a weak position of technology, aim to formulate relatively strict cyber security regulations to acquire more space for autonomous development in the cyber field and protect national cyberspace sovereignty. Western developed countries have the authority to establish cyber technology standards, but they secretly apply double standards. They advocate for "Internet freedom" and "open cyberspace" to facilitate their violations of other nations' sovereignty via the Internet to reap benefits. However, developing countries have to act according to Western nations' access thresholds and standards because of the late start in network construction and lack of substantial construction expertise and technology accumulation. Therefore, the majority of developing countries, represented by China and Russia, are not opposed to "Internet freedom", but the use of "Internet freedom" by Western developed countries to exercise "long-arm jurisdiction" and interfere in the domestic affairs of other countries, which seriously violates the purposes and principles of the UN Charter.

2.2. The international community has conflicting values on cyberspace.

Humanity has gradually transitioned from an industrial culture to an information-savvy society with the advent of the Internet. Several ideologies have interacted with cyberspace in this process, resulting in diverse values, and countries have varying Internet-related technological and developmental levels. As a result, the international community has various perceptions and perspectives regarding the openness and freedom of the Internet, making it challenging to create consensus on the rules of international cyberspace administration. For instance, in the process of combating COVID-19, countries such as China, Singapore, and Italy have utilized digital tracking technology to prevent the spread of the virus effectively. Apple has therefore stated that it would collaborate with Google to develop an app that will notify mobile phone users if they have had contact with a positive patient during the previous 14 days. The application will decrease patient exposure and successfully contain the outbreak's spread. However, this action is viewed as violating residents' right to privacy.

Western countries, such as America and Britain, view the Internet as a tool for disseminating human rights and are eager to promote online freedom of expression. Any discussion of legal regulation of cyberspace will inevitably be elevated to the level of an infringement of "internet freedom." Some countries, such as China and Russia, consider the Internet an extension of the natural world, and it should obey the laws of the actual world rather than an unfettered emphasis on online freedom. Therefore, as there are conflicting values, it is challenging to create a worldwide consensus, and even when the international agreement has been presented, it has begun to disappear before its implementation. For instance, "technological neutrality," initially proposed by the European Union and its member states in a regional context, was inserted into the draft report by the UN Working Group in March 2020. However, it has not yet played a role in international cyberspace governance. Meanwhile, due to the Snowden case, countries worldwide lack trust in imported Internet products and have enhanced security examination of their products. Some even establish market access barriers for foreign Internet companies.

2.3. Cyberspace becomes the new worldwide battlefield.

The Internet was initially a US military project with a political complexion. As the Internet has progressed and begun to interact with the actual world, it has become the centre of worldwide competition. In a world where countries push Artificial Intelligence, the risk of military, economic, and political cybersecurity threats to countries has increased dramatically. Although cyber-attacks are not as powerful as traditional physical attacks in terms of force and actual damage, they have a more comprehensive range of targets. They can achieve a broader reach than physical attacks, as shown by the Stuxnet virus, which infected more than 45,000 websites worldwide when it was discovered. As a result, countries continuously enhance their cyber assault capabilities and cyber security defences as they negotiate an international cyberspace order. Some Western developed countries are even pursuing a Cold War mentality and double standards in global cyberspace security governance to stifle the development of cyber technology in other countries. They display signs of a desire to make cyberspace the "main battlefield" of a new hegemony.[7]

In addition, due to the virtual nature of cyberspace, cybercrimes always leave no evidence and are difficult to trace back to their source, making them highly concealable. From the objective view, a network system with total security does not exist. Therefore, a cyber-attacker could launch an attack on the system at will as soon as he discovers a vulnerability. Even with thousands of security professionals on the defence, it is hard to stop the attack immediately. With cyber-attacks being easy to launch and hard to fight against, the threat to cyberspace security is growing in prominence. When countries are involved in cyber-attacks, the safety hazard intensifies. In this context, many countries have devoted more resources to competing for the right to establish the rules of cyberspace security governance, focusing more on how to take the lead in the new technological revolution and industrial transformation than on achieving global security governance. For instance, the purpose of "The Clean Network" of the US is to protect its technological monopoly and limit China's technological advancement. The expansion of international rivalry and games into cyberspace has slowed the development of an international security mechanism and could not gain a breakthrough.

3. Future international cyberspace security governance choices

3.1. The international community should actively play the the United Nations "dual-track system" role and establish globally acceptable behavioural norms.

Currently, the conflicting values of international governance in cyberspace have caused a delay in forming an international consensus, and even the proposed international agreement is gradually collapsing. The UN "dual-track system" was established to break the logjam in global cyberspace security governance. Its core mission is to seek international consensus through negotiation, to discuss and formulate norms of conduct for international cyberspace security governance, to build a rules-based cyberspace order, and to provide the UN member states with guidelines for action. Today, the United Nations is the world's most authoritative and representative intergovernmental organization. Therefore we should maximize the function of the United Nations dual-track system and actively encourage new advances and effectiveness in cyberspace world governance.

3.2. The international community should promote the reginal formation of rules of cyberspace governance.

Regarding the current attitude of the international community on international cybersecurity governance, it is tough to reach a worldwide consensus shortly. However, the issue of cybersecurity governance needs to be addressed immediately. The international community could focus on finishing regional international accords. It is more practical and efficient to reach a regional consensus than a worldwide agreement. It is also more convenient for countries with similar interests to work together. For instance, the United States has stated that it will pursue more substantive bilateral agreements without abandoning multilateral consensus. International organizations have already implemented methods and developed several regional accords about cyberspace security governance. In September 2011, China, Russia, Tajikistan, and Uzbekistan, four members of the Shanghai Cooperation Organisation, jointly submitted an International Code of Conduct for Information Security to the UN. In December 2020, the European Commission released its most recent Cybersecurity Strategy as an objective and guiding principle for the EU Digital Decade.

3.3. The international community should adhere to the "multilateralism" legislative path.

Currently, one of the primary reasons for the delay in gaining a breakthrough in international cyberspace governance is the Western developed countries, led by the US, have taken a "unilateralist" legislative approach to construct an international cyberspace security order. They hope to build norms and codes that maximize their interests as much as possible by using their technological advantages. Judging from the current legislative achievements through the implementation of "unilateralism", the norms in cyberspace formulated by Western developed countries are highly unfair and ignore the interest wishes of most developing countries, such as "removing technical barriers" and "protecting cyber sovereignty". However, cyberspace is worldwide, and Western counties have no right to deprive the opportunities of developing countries of participating in cyberspace international governance. Regarding the current issues encountered in implementing global management in cyberspace, for instance, how can rules of existing international law be applied to cybersecurity governance? How can the framework of "norms of responsible state behaviour" be completed?[8] Global cyberspace security is a problem for the international community, and no country can be immune from it. Therefore, cyberspace governance should be examined and resolved by the world community based on international consensus, not by the Western developed countries.

4. Conclusion

Currently, cyberspace has become a new arena for international rivalry. All nations aspire to adopt cybersecurity rules of conduct that align with their national interests, resulting in the delay of the governance process. Whereas as the Internet evolves, cyber threats become increasingly severe. It is imperative to implement a global cybersecurity policy. As a result, the international community should fully use the UN's "dual-track system" as a global platform to develop universally accepted norms of behaviour. Furthermore, reaching an international consensus in the short term is difficult, but cyberspace governance needs to be addressed immediately. The international community could shift its focus to promoting regional norms of cyberspace governance. Last but not least, it is vital to adhere to the legislative road of "multilateralism" and develop cyberspace security standards that reflect the interests and needs of most nations.

References

[1] Wang Guiguo. Rules of international governance in cyberspace and their application [J]. China Law Review, 2021(02):15-29.

[2] Tang Runhua, Li Zhi. A new path for global cyberspace governance: the UN "dual-track" platform and China's participation [J]. DOI:10.13628/j.cnki.zjcmxb.2022.03.009.

[3] Tian L. The path choice of China's participation in the construction of international law in cyberspace from the perspective of international security [J]. Yunnan Social Science, 2021(06):93-105.

[4] Huang Zhixiong. The application of international law in cyberspace: the game of rules in the construction of order [J]. Global law review, 2016, 38(03):5-18.

[5] Liu Biqi. On the basis and legitimacy of the application of international law in cyberspace [J]. Theory Monthly, 2020(08):109-119. DOI:10.14180/j.cnki.1004-0544.2020.08.012.

[6] Tang Shuchen, Yu Long. Exploring the practice and prospect of building an international governance pattern in cyberspace [J]. China Information Security, 2022(04):70-74.

[7] Yang Xiaoqiang, Li Ruohan. International cyberspace security governance: dilemmas, reflections and countermeasures [J]. Henan Social Science, 2022, 30(06):101-109.

[8] Liu Jinhe, Yang Le. The game focus and development trend of the dual-track process under the framework of the United Nations [J]. China Information Security, 2021(09):81-84.