A brief discussion on the development of cyberspace regulation

Chengxiang Wen[1,a], Jiaoyi Wu[2,b,*]

[1]School of Digitalized Intelligence Engineering, Hunan Sany Polytechnic College, Changsha, China

[2]Law School Peking University, Beijing, China

[a]775364962@qq.com, [b]412677236@qq.com

*Corresponding author

Keywords: International law; cyberattacks; cyberspace regulation; DDOS attacks

Abstract: This paper introduces the DDos attack in Ukraine in early 2022 and puts forward the need for international cooperation regulation of cybersecurity. The draft resolution on information security submitted by Russia at the United Nations General Assembly in 1998 introduced the development of an international rule of law framework in cyberspace led by the United Nations, and briefly analyzed the different attitudes of different countries towards cyberspace regulation. Next, the "gray field" of the current concept of international law in cyberspace is briefly introduced, the concept of sovereignty in cyberspace is briefly explained, and finally the further construction of the international legal law system in cyberspace is prospected in the twists and turns.

1. Introduction

On January 14, 2022, during the Russia-Ukraine crisis, a DDoS cyberattack paralyzed more than a dozen Ukrainian government websites.[1]According to Ukrainian officials, about 70 government websites, including the Ministry of Foreign Affairs, the Cabinet of Ministers and the Security and Defense Council, were attacked.[2] On February 15, another major DDoS attack paralyzed several government and banking services in Ukraine, which The New York Times described as "the worst in Ukrainian history." [3] It can be said that with the development of science and technology, cyberspace has gradually become another stage for conflicts of national interests. Before the start of the Russian-Ukrainian ground conflict, the "cyber war" between the two sides is likely to have already begun, but such an invisible battlefield is often not very noticeable.

2. The needs of international laws and regulations in cyberspace

"Cyberspace has become the fifth space for human activities after land, sea, sky and outer space. One of the consequences of this is that the security and stability of global cyberspace has increasingly become an important issue affecting the development of the international system. "[4]

Nowadays, the daily life and work of people in various countries have been deeply embedded in cyberspace, various large-scale transnational network platforms are lined up, and global economic activities occur frequently in cyberspace....According to the International Telecommunication Union, 4.9 billion people worldwide will already use the Internet by 2021[5]. It can be said that the Internet can be said to be synonymous with innovation and prosperity, bringing universal benefits around the world.

In the Oxford English Dictionary, cyberspace is defined as "the conceptual environment for communication through computer networks." It can be argued that cyberspace is based on the Internet, but it is a broader concept than the "Internet". [6] The construction of such a "cyberspace" beyond the physical space can be divided into two layers: on the one hand, at the physical level, Internet network providers build sites around the world to exchange traffic, and the connected Internet cables penetrate land and cross the sea; On the other hand, in the virtual space, information is propagated in the form of segmented packets based on various communication protocols, trying to reach the destination through the fastest path. [7]

  DOI: 10.25236/icfmhss.2023.050

But there are pros and cons, and the Internet is also a source of danger—hackers, the dark web, viruses, privacy leaks, cybercrime, cyberterrorism—and these dangers that spread along the cable pose serious challenges to individual lives, global economic, social, political, and public safety. The aforementioned DDoS attack, known as Distributed Denial of Service attack or more figurative "flood attack", is a common network attack method. By exhausting the network or system resources of the target computer, the service is temporarily interrupted or stopped, making it inaccessible to normal users[8], as was the case with the large-scale cyberattack in Estonia in 2007. In addition, another common cyberattack method is malware intrusion, such as the "Stuxnet" attack that swept the world in 2010 and was the hardest hit by Iran. Cyber attack methods are actually endless, and there are often complex international politics and interest entanglements behind them, which bring serious harm to the social, economic and security of the attacked countries.

An Internet fraught with dangers undoubtedly needs to be managed, and the question is who will manage it and how.

Freedom was once widely considered the essence of the Internet, which has always been fraught with confrontations between sovereignty and freedom. In 1996, John Perry Barlow issued the Declaration of Cyber Independence, and in response to the Communications Decency Act of the United States, he impassionedly declared that governments were "disgusting iron-blooded giants", unpopular with the free-spirited Internet, and that governments "have no sovereignty" in cyberspace.[9] In the same year, the Stanford Law Review published an article defending the free Internet, which strictly adhered to the correspondence between the physical boundaries of territory and legal sovereignty, arguing that the Internet, as a new field of human activity, would create its own new laws and legal systems, and therefore did not apply the traditional concept of state sovereignty. [10]

Of course, such a romantic "cybertopian" liberal idea was later opposed by more scholars, such as Jack L. Goldsmith, who directly criticized this kind of network anarchism.[11] and Lessig pointed out that there is a fallacy of "what is and what should be", that there is no framework that can determine the nature of the Internet, that the Internet is regulated, and that regulation is necessary to protect fundamental freedoms. The more general view is that cyber sovereignty is a natural extension of traditional state sovereignty in cyberspace, thus emphasizing the isomorphism between cyberspace and real space. [12]

Therefore, there is no doubt that the government has the power to manage cyberspace, and the transnational and borderless nature of the network makes it impossible for its governance to be isolated countries. A secure, stable, prosperous and peaceful cyberspace requires the joint efforts of governments, international organizations and even large multinational enterprises to regulate it, and the establishment of a specific governance system is a tortuous process of continuous development.

3. The development of international laws and regulations in cyberspace

The United Nations has been an important venue for the international cybersecurity debate, and the UN cybersecurity negotiations can be divided into political-military factions focused on cyberwarfare and economic factions focused on cybercrime. [13] The former involves UN bodies such as the First Committee of the UN General Assembly, the International Telecommunication Union (ITU), the United Nations Institute for Disarmament Research (UNIDIR) and the Counter-Terrorism Implementation Task Force (CTITF), while the latter includes the Third Committee of the UN General Assembly, the UN Economic and Social Council (ECOSOC), the United Nations Office on Drugs and Crime (UNODC), and the United Nations Interregional Crime and Justice Research Institute (UNICRI).

In 1998, Russia first introduced a draft resolution on "The impact of achievements in the field of information and telecommunications on international security"at the UN General Assembly, calling on States to warn of the military use of information technology and urging the Entente countries to help examine existing or potential threats in the field of information security; This time the draft was adopted in 1999.However, Russia's subsequent attempts to push for an international agreement were resisted by the United States and some European countries, and Russia was the sole sponsor of

the proposal for many years. After the resolution was voted against by the United States in 2005 by the only recorded vote , by 2006 Russia's actions were supported by China, Armenia, Belarus and other countries, and in the following years, the number of co-sponsors continued to rise; The latest General Assembly resolution was made at the end of December 2021.

Under the influence of the Russian proposal in 1998, the United Nations established the first United Nations Group of Experts on Information Security (GGE) in 2004 to promote the development of international cyber norms. GGE is the main mechanism led by sovereign states in the field of network specification construction, and the resulting cyberspace norms have high legitimacy and authority. [14] So far, the GGE has been held for a total of six sessions, of which the discussions in 2012-2013 and 2014-2015 have made great breakthroughs, and the landmark establishment of the application of international law, especially the UN Charter, in cyberspace.

The latest GGE report is important because the GGE countries did not reach a consensus in the fifth edition of 2016-2017. [15] In a report published in 2021, the GGE confirmed that international humanitarian law (IHL) applies to cyber operations during armed conflict (but further questions are how IHL specifically regulates cyber operations during armed conflict). The 2021 report also details the peaceful settlement of disputes, clarifying the obligations under Article 2.3 and Chapter VI of the UN Charter and the means of Article 33 of the UN Charter. The 2021 report further elaborates the prohibition of intervention, noting that interventions can be direct or indirect, such as ICT intervention. The GGE also highlighted cooperation and transparency measures, encouraging countries to clarify their positions and gain support through regional and bilateral exchanges of views.

On the basis of acknowledging the 2021 GGE report, the GGE report also has shortcomings, such as the report continues to recognize sovereignty, including the requirement to respect the sovereignty of other countries, but still does not clearly characterize it as binding rules, nor does it clearly distinguish between remote cyber operations that violate sovereignty. For example, this report, which builds on 2015, continues to focus on the use of ICT by one country against another country, such as "clandestine information campaigns facilitated by malicious use of ICT to affect the processes, institutions and overall stability of another country", but still does not explicitly address any countermeasures. [16]

Of course, as noteworthy as the GGE is the Open Working Group (OEWG), which has been established for two terms in 2018 [17] with the goal of establishing international rules and improving the trust mechanism, and the OEWG has included many non-governmental international organizations and large enterprises in civil society groups, such as Microsoft and Kaspersky. The OEWG and GGE are considered to be a "dual-track" model under the United Nations, jointly advancing the rule-making of cyberspace. [18]

If the breakthrough of the 3rd and 4th GGE lies in clarifying the general application of the UN Charter and international law in cyberspace, the Internet is not an extrajudicial place for international regulation, and existing mature solutions can be used to solve new problems of the global Internet; The confusion of the fifth and sixth GGE lies in the slow progress in determining specific principles and standards for the application of rules due to different opinions among countries - but this is almost an inevitable process of the establishment of any rule of international law. After failing to reach consensus at the fifth GGE, the sixth GGE shied away from the spotlight and focused on developing its non-binding norms to establish a framework for responsible behavior in cyberspace–it is believed that, over time, some norms are likely to be recognized by many countries as binding law, or crystallized into customary international law or authoritative interpretations of established rules.

Promoting an international rule of law framework in cyberspace is by no means easy. Different countries have different attitudes towards international laws and regulations in cyberspace, which is not only related to the level of network technology of various countries, but also closely related to their own cultures, beliefs and social values, and is also influenced by the interest game between countries and groups.For example, the West represented by the United States claims to value privacy, freedom of speech, and freedom of information; China is actually concerned about national

cyber sovereignty and hopes to play an important role in the formulation of global cyber rules. In fact, both China and the West have repeatedly portrayed each other as potential or actual adversaries in cyberspace, with common areas of contention such as the application of sovereignty to cyberspace, the militarization of cyberspace, and the legality of cyberespionage. But in detail, these camps are not absolutely torn, but generally show a convergence trajectory; In order to build an international rule of law framework in cyberspace, what is needed is a better understanding of the potential for convergence and a focus on positive developments. [19]

4. The "Grey Zone" of International Cyber Law: Taking the Concept of Sovereignty as an Example

Michael N. Schmitt, a key compiler of the Tallinn Handbook, cited the 2015-2016 Democratic Party email portal in the United States as an example in 2017, pointing out that there are many poorly defined principles or rules in international law in cyberspace that are governed by competitive interpretation, and that countries that benefit from "asymmetric laws"are veterans skilled in these "gray areas"; In this regard, the article proposes some gray areas (such as sovereignty, due diligence, use of force and self-defense, etc.) caused by differences of opinion in the international legal system of cyberspace, and Schmidt believes that relying on national legal conviction can narrow this gray area. [20] This article briefly elaborates on sovereignty as an example.

China has always emphasized the concept of cyber sovereignty in international regulations in cyberspace, but the West, represented by the United States, tends to portray China's emphasis on cyber sovereignty as a threat to Internet freedom[21]. But Chinese scholars believe that this is actually because the United States has been controlling the Internet implicitly or explicitly at different times, and the US government has always believed that the Internet fundamentally belongs to the United States itself. [22] In fact, although the existence of sovereignty in cyberspace is now widely established internationally, different countries have different conclusions on the specific understanding, application and specific focus of this concept. For example, Schmidt's sovereignty rule should refer to how to determine that unlawful cyber attacks constitute infringement of sovereignty, which is different from the Chinese of China.

Schmidt affirmed state cyber sovereignty, and he focused on two gray areas in the norms of cyber sovereignty, one is that "sovereignty is a principle of international law guiding the interaction of states, not a binding rule", which means that a violation of sovereignty only constitutes a violation of international law to the extent that it constitutes a prohibition on interference or the use of force[23]. The second is the more mainstream view that sovereignty itself is an independent rule that can be violated, and that the violation of sovereign rules will have consequences under the law of State responsibility.

In the Tallinn Manual 2.0, it is argued that as long as there is a temporary loss of function caused by a cyberattack, even if there is no physical damage, it is a violation of sovereignty, but the problem is that reaching a more precise standard of determination is controversial. Schmidt argues that this is a gray area in the concept of sovereignty, leaving uncertainty about the determination of cyberattacks such as DDoS and ambiguity about how the attacked country will react. Schmidt's solution is to rely on national legal conviction to clarify the problem–although this ambiguity leaves some room for manoeuvre for all countries, he still believes that legal clarity contributes to international stability; The brighter the red line warning of international law, the less chance that countries will exploit gray areas to create instability.

The direction of establishing clear rules of international law on the Internet is indeed ideal, but the fact may be the same as the slow promotion of the GGE, under the large framework, countries can reach an agreement, but in the details, it is easier to diverge due to the interests and normative preferences of countries, and it is difficult to form a consensus. From the results of the latest GGE, it appears that insisting on consultation and promoting non-binding rules may be one direction; But it is also possible, as some have done since the failure of the fifth GGE, that international regulation of cyberspace will shift from ambitious global initiatives to regional agreements between

"like-minded nations" – and we are likely to see a fragmented structure of international norms in cyberspace. [24]

5. Future prospects

Despite the re-reaching of consensus at the sixth GGE, the United States still issued the so-called Declaration on the Future of the Internet on April 28, 2022, local time and 60 other governments. [25] This US approach is widely regarded as the latest example of splitting the Internet, squeezing out China and Russia, and provoking confrontation in cyberspace, adding twists and turns to the common governance of the global Internet.

However, the worldwide prosperity and co-governance of cyberspace is a matter of a long-term scale - whether it is technology itself, as well as the politics, society, and laws of various countries, it needs to be constantly improved or even transformed, and it cannot be smooth sailing. If the former liberal utopia can still inspire today's world, it may be the idealistic hope that cyberspace truly belongs to the whole world on an equal footing, rather than further competing for "network power" in the new era after competing for land and sea power.

Only by understanding each other's similarities and differences and respecting each other's different concepts and institutional frameworks for the rule of law with a truly free, open and inclusive attitude can we jointly promote the vigorous development of cyberspace and establish a reasonable, equal and just Internet international governance framework. Finally, "cyberspace is a space for common human activities, and the future of cyberspace should be jointly controlled by all countries in the world, and all countries should strengthen dialogue and cooperation and work together to build a community with a shared future in cyberspace."

References

[1] "Ukraine cyber-attack: Government and embassy websites targeted", BBC News, 2022-01-14, available at https://www.bbc.com/news/world-europe-59992531. Last visited: April 29, 2021.

[2] Pavel Polityuk, Steve Holland, "Cyberattack hits Ukraine as U.S. warns Russia could be prepping for war", Reuters, 2022-01-14, available at https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/.

[3] Valerie Hopkins: "A hack of the Defense Ministry, army and state banks was the largest of its kind in Ukraine's history", The New York Times, 2022-02-15, available at https://www.nytimes.com/2022/02/15/world/europe/ ukraine-cyberattack.html.

[4] Qu Yantao, "Wuzhen Network Affairs: Global Experts Discuss the Security of the Fifth Space," Xinhuanet, December 19, 2015, http://www.xinhuanet.com/mil/2015-12/19/c_128547220.htm.

[5] ITU website: https://www.itu.int/itu-d/reports/statistics/facts-figures-2021/.

[6] Lawrence Lessig, Code 2.0: Law in Cyberspace, translated by Li Xu and Shen Weiwei, Tsinghua University Press, 2009, p. 10.

[7] Kriangsak Kittichaisaree, Public International Law of Cyberspace, Springer, 2017, p.3.

[8] Wikipedia: https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_DoS. .

[9] John Perry Barlow, A Declaration of the Independence of Cyberspace, Duke Law & Technology Review, Vol 18:1, p.5-7 (2019) (Reprinted).

[10] David R. Johnson, David Post, Law and Borders: The Rise of Law in Cyberspace, Stanford Law Review, Vol 48:5, p. 1367-1402 (1996).

[11] Jack L. Goldsmith, Against Cyberanarchy, University of Chicago Law Review, Vol. 65:4 , p.1199-1250 (1998).

[12] Timothy S. Wu, Cyberspace Sovereignty The Internet and the International System, Harvard Journal of Law and Technology, vol 10:3, 647-666 (1997)

[13] Tim Maurer, Cyber norm emergency at the United Nations - An Analysis of the Activities at the UN Regarded Cyber Security, Discussion Paper, 2011-11, Science, Technology, and Public Policy Program, Belfer Center, Harvard Kennedy School, September 2011

[14] Lu Chuanying and Yang Le: "On the Operational Mechanism of the United Nations Information Security Government Expert Group in the Process of Formulating Cyberspace Standards", published in Global Media Journal, Volume 7, Issue 1, 2020.

[15] Tikk E, Kerttunen M, The allowed promise of the UN GGE: An autopsy and ecology [J] New York, 2017

[16] Michael N. Schmitt, The sixth United Nations GGE and international law in cyberspace, Just Security, New York University School of Law, June 10, 2021, available at https://www.justsecurity.org/76864/the-sixth-united-Nations-gge and international law in cyberspace/

[17] https://www.un.org/disarmament/open-ended-working-group/ ; The second OEWG was established in December 2020 by Resolution A/RES/75/240, with a renewal period of 2021-2025, https://meetings.unoda.org/meeting/oewg-ict-2021/ .

[18] Valentin Weber, How to Strengthen the Program of Action for Advising Responsible State Behavior in Cyberspace, Just Security, 2022-10, available at https://www.justsecurity.org/80137/how-to-strengthen-the-programme-of-action-for-advancing-responsible-state-behavior-in-cyberspace/.

[19] Zhixiong Huang, Kubo Ma čá k, Towards the International Rule of Law in Cyberspace: Controlling Chinese and Western Approaches, Chinese Journal of International Law, Vol 16:2, P.271-310 (2017)

[20] Michael N. Schmitt, Grey Zones in the International Law of Cyberspace, The Yale Journal of International Law Online, Vol 42:2, p.1-21 (2017)

[21] Michael N. Schmitt, Liis Vihul, Sovereignty in Cyberspace: Lex Lata Vel Non?, AJIL Unbound , Vol: 111 , p. 213 - 218 (2017)

[22] Liu Han, "Domain Name System, Cyber Sovereignty and Internet Governance: Historical Reflections and Their Contemporary Enlightenment," Sino-Foreign Legal Science, No. 2, 2016.

[23] Gary P. Corn, Robert Taylor, Sovereignty in the Age of Cyber, American Journal of International Law Unbound, Vol:111, p.207-212 (2017).

[24] Anders Henriksen, The end of the road for the UN GGE process:The future regulation of cyberspace, Journal of Cybersecurity, Vol 5:1,p. 1-9 (2019).

[25] The White House, “FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet”, 2022-4-28, available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/ 28/ fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/