ARE THERE INTERNATIONAL RULES GOVERNING CYBERSPACE?

Guiguo Wang*

Abstract: Cyberspace is open and operates across borders. Aware of significant challenges that this poses to the international community, the UN has adopted several resolutions calling for the use of cyberspace in accordance with the UN Charter. It also set up a government expert group to deal with cyberspace issues. Yet, due to a lack of consensus, reports of the expert group could not be endorsed by the UN. The rapid integration of cyberspace into our lives necessitates regulation of its operation. The question is which rules may govern the cyberspace. This article argues that the UN Expert Group's reports clearly show that there is a consensus among the international community that cyberspace is subject to international law including the UN Charter. It also argues that agreements reached by states at regional and bilateral levels, customary international law and existing rules of international organisations such as the World Trade Organization (WTO) constitute a body of cyberspace governance rules. In accordance with the relevant International Court of Justice (ICJ) judgments and International Law Commission's (ILC's) conclusions on identification of customary international law, it is the view of this author that customary norms applicable to cyberspace may be constituted through practices of the user states as special customary international law rules and that practices of Internet companies and entities, despite their non-binding nature on states, may contribute to the confirmation of the existence of such customary rules.

Keywords: *cyberspace; cybersecurity; sovereignty; Internet; big data; customary international law; digital economy; information and communications technology; WTO*

I. Introduction

The advancement of science and technology, especially the rapid development of cyberspace including the Internet, big data, the Internet of Things, cloud computing and telecommunications technology has greatly facilitated the process of

* Guiguo Wang, LLM (Columbia), JSD (Yale), is University Professor of Law, Zhejiang University and President of the Zhejiang University Academy of International Strategy and Law, Hangzhou, China. The author may be contacted at White House, No.51, Zhijiang Rd, Xihu District, Hangzhou, People's Republic of China. gwang29@tulane.edu.

[(2021) 8:2 JICL 357–384]

globalisation, making cyberspace the fifth largest domain after land, sea, air and space.[1] The widespread use of information and communications technology (ICT) as the backbone of cyberspace clearly shows the value of data. Since the 1970s, cross-border data flow has gradually emerged as a new economic model.[2] The widespread application of cyberspace technologies has made efficient and rapid transmission of big data possible; and this trend continues to grow exponentially. Through the medium of network 1/0-byte transmissions, the direct effect of this digitalised world economy has reshaped the world supply chains and distribution networks, significantly reducing the cost of transactions and enabling small and medium-sized enterprises (SMEs) to compete with traditional transnational corporations (TNCs). The effective use of cyberspace may bring enormous benefits to human society and economic development; conversely, it may also cause adverse effects.

The resultant challenge is to make effective use of the potential of cyberspace while avoiding any negative impact on human society. Likewise, there is a need for an effective legal mechanism to prescribe rights and obligations of the parties concerned. Where such a mechanism is absent, which norms and rules are needed and who are in a position to formulate such rules and norms?

In order to address the aforementioned questions, Part II of this article will briefly examine the technological aspect of cyberspace and discuss the main novel challenges it poses to the world. Section III will analyse the legal challenges arising from the rapid advancement of cyberspace technology to the international community. The most important challenges are cyber sovereignty and cybersecurity, whose very nature requires international cooperation for a solution. Section IV will examine the efforts made by the international community in formulating rules to regulate cyberspace and, in absence of agreements among states, whether customary international law could apply to cyberspace. It argues that the essential

1 "Fifth Domain" was first proposed by the *Economist* in 2010. The concept was officially recognised by the United States Department of Defense (hereinafter referred to as "US DoD") in 2011. The US DoD indicated in the Department of Defense Strategy for Operating in Cyberspace that ". . . . . DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests". "War in the Fifth Domain" *The Economist* (1 July 2010), available at https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain (visited 11 July 2021); "Department of Defense Strategy for Operating in Cyberspace" *Department of Defense* (July 2011) 5, available at https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (visited 11 July 2021). UNESCO defines cyberspace as "A world-wide virtual space, different from real space, with many sub-communities unevenly distributed using a technical environment—first of all the Internet—in which citizens and organizations utilize information and communication technology (ICT) for their social and commercial interactions". "Cyberspace", *UNTERM*, available at https://unterm.un.org/unterm/display/record/escwa/na?OriginalId=28efe7cc-a250-4922-b512-61f843afb1b5 (visited 11 July 2021). In this article, "cyberspace" refers to the Internet, information technology, data, the Internet of Things, etc., and "cyberspace governance" refers to the collection of principles, rules and standards related to the operation of cyberspace, especially cross-border cyber activities.

2 The Council of Europe adopted two resolutions on cooperation among its member states for protection of personal information: Council of Europe (Committee of Ministers), "Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector" (26 September 1973); and Council of Europe (Committee of Ministers), "Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector" (20 September 1974).

principles of international law including the Charter of the United Nations (UN Charter) are applicable to cyberspace and that existing customary rules constitute the contents of cyberspace governance. Section V will examine the steps taken by states and norms proposed by private entities in regulating cyberspace-related activities, which were done against the background that the use of cyberspace has become indispensable. Section V proceeds to argue that state practices and norms proposed by private entities will contribute to the formulation of international rules including the formation of customary law governing cyberspace. Section VI will examine the prospects of cyberspace governance by asserting the binding effects of international law. It argues that state sovereignty and cooperation among states and other parties are the essential rules governing cyberspace. It also argues that following the International Court of Justice (ICJ) and United Nations International Law Commission (ILC) practices, particular customary rules can be formulated through the practices of states which are important users of cyberspace. As for the future, Section VI argues that protection of privacy and personal and social data should be emphasised in international rulemaking relating to cyberspace.

II. Cyberspace Posing New Challenges

Cyberspace is inseparable from data, which is referred to as "oil of the 21st century"[3] or "currency of the digital economy".[4] The innovation in data collection, processing, analysis, use, storage and flow has promoted the development of international economic transactions and exchanges and has made the digital economy, with e-commerce as its major component, an independent economic sector.[5]

The invention of the Internet technology can be traced back to the 1930s, when the application of the technology was set off during the Second World War.[6] Technology began to flourish during the Cold War when the Western Bloc found it necessary to develop a communication system that could survive the first strike of

3 Shannon Tellis, "Data is the 21st Century's Oil, Says Siemens CEO Joe Kaeser" *The Economic Times* (24 May 2018), available at https://economictimes.indiatimes.com/magazines/panache/data-is-the-21st-centurys-oil-says-siemens-ceo-joe-kaeser/articleshow/64298125.cms?from=mdr (visited 11 July 2021).

4 William D Eggers, Rob Hamill and Abed Ali, "Data as the New Currency" *Deloitte Insights* (24 July 2013), available at https://www2.deloitte.com/us/en/insights/deloitte-review/issue-13/data-as-the-new-currency.html (visited 11 July 2021).

5 Unlike the traditional economy, where information flows are in physical form, such as cash, cheques, and bills of lading, information flows in digital economy are binary codes stored in computers. See Don Tapscott, *The Digital Economy: Rethinking Promise and Peril in the Age of Networked Intelligence* (20th Anniversary ed., McGraw Hill Education, 2015) p. 16.

6 Vannevar Bush is said to be the first person to introduce the concept of the Internet in a paper entitled "As We May Think" that was completed in 1939 but published only after the end of the Second World War. See Vannevar Bush, "As We May Think" *The Atlantic* (July 1945), available at https://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/ (visited 11 July 2021); John Naughton, *A Brief History of the Future: The Origins of the Internet* (London: Weidenfeld Press, 1999) p. 214.

a nuclear attack. The initial Internet system was launched in 1972,[7] solely serving military purposes. The system became accessible to the general public in the early 1980s and was commercialised in 1995.[8] In just over two decades, the Internet has become an inseparable part of human society playing a vital role in the social development and making the world ever increasingly globalised.

Being open and borderless, cyberspace, including the Internet, cannot be effectively regulated by domestic law. The United Nations Educational, Scientific and Cultural Organization (UNESCO) describes Internet governance as "the complementary development and application by governments, the private sector, civil society and the technical community, in their respective roles, of shared principles, norms, rules, decision-making procedures, and activities that shape the evolution and use of the Internet".[9]

In view of this global reach of Internet governance, the UNESCO advocates an open, transparent and inclusive approach to Internet governance based on the principle of openness, encompassing the *freedom of expression*, respect for privacy, universal access and technical interoperability. To date, this has been one of the most comprehensive elaborations on cyberspace governance. It also illustrates that the world has shifted its focus from the Internet-related critical information infrastructure, such as the domain name system and websites, to the need for effective regulation. This is in line with the progression of the Internet that has entered the political, economic and social spheres of all states. With this development, the scope and content of international governance of cyberspace must expand into every aspect of human life, for example market access, security and trust, digital use and analysis, Internet of Things, blockchain technology, human rights, privacy, public health and public safety. In its *World Development Report 2016: the Digital Dividend*, the World Bank made the following observation:

> The Internet and related technologies have reached developing countries much faster than previous technological innovations. For Indonesia to recap the benefits of steamships took 160 years after their invention and for Kenya to have electricity, 60 years; but for Vietnam to introduce computers, only 15 years. Mobile phones and the Internet took only a few years. More households in developing countries own a mobile phone than

7 The Internet system was first referred to as Advanced Research Projects Agency Network (ARPANET), which "was built with astonishing speed. By 1972, the network was essentially complete; the 15 original sites were all connected and operational and a major public demonstration of the system was held in Washington, DC in the Autumn of that year". See John Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology" (2016) 1 *Journal of Cyber Policy* 5, 8.

8 *Ibid*., 5.

9 UNESCO made this statement at the very beginning of its Internet Governance website. See "Internet Governance" *UNESCO*, available at https://en.unesco.org/themes/internet-governance (visited 11 July 2021).

have access to electricity or improved sanitation. Greater Internet access has led to an explosion in the production and consumption.[10]

Openness and other characteristics of cyberspace pose serious challenges to the existing international mechanisms. For example Internet companies process large volumes of personal data for commercial purposes. Although such processing underpins digital economy and digital transactions, it inevitably involves issues such as those relating to privacy, cybersecurity, digital infrastructure construction and balanced capacity building. Moreover, the diversification of digital technologies, including cloud computing, the Internet of Things, artificial intelligence and quantum computing and so on, brings new challenges to the international community. This is inevitable because economic development depends on technological advancement. In today's highly globalised world, there must be coordination and cooperation among governments, private enterprises and other entities, if states desire economic development and scientific and technological innovation. In fact, international cooperation is essential even in sanctioning or curbing a state or an entity. For instance the Trump administration which always stressed "America First" had to collaborate with its allies—for instance it used the Five Eyes alliance to suppress Huawei, an ICT company headquartered in China.

Advances in Internet technology have led to an infinite expansion of the virtual space, allowing anyone to instantly transfer data stored in a mobile phone or computer to a remote storage, such as cloud. In light of the transnational nature of cloud storage, some advocate "data exception", that is the nature of cloud storage decides that it is not subject to the norms of international law based on territorial jurisdiction. Others propose that as data has both physical and intangible characteristics, it is justifiable for states to exercise jurisdiction over it.[11] For decades, states have exercised jurisdiction over intangible things such as intellectual property (IP) rights. Such jurisdiction may be exercised over the owner or actual disposer of such intangible property. The same principle could be applied with regard to the exercise of jurisdiction over data. Judicial practice in some states too supports this approach.[12] Therefore, where a state exercises jurisdiction over the data stored in cloud, it needs to assert jurisdiction based on the geographic location of data storage, the domicile of data controller, the place of the offence, the residence of the victim or the nationality of the offender(s). The characteristics of cloud storage do indicate that more than one state may exercise jurisdiction at any given time, which constitutes a new challenge to the international community as the contemporary

10 See The World Bank, "World Development Report 2016: Digital Dividends" *The World Bank* (2016) 5, available at https://www.worldbank.org/en/publication/wdr2016 (visited 11 July 2021).

11 See Andrew Keane Woods, "Against Data Exceptionalism" (2016) 68 *Stanford Law Review* 729, 734. This is further explained in Part II B "The Reality: Data is Not So Different". *Ibid*., 755–758.

12 For example in *U.S. v Bank of Nova Scotia* 740 F2d 817, 11th Cir (1984), the US Federal Court of Appeals ruled that the Canadian bank could not refuse to submit the data on the grounds that the data was held in a foreign country and could not be submitted under the laws of that foreign country.

international rules may not be readily applicable to the cyberspace including cloud storage.

III. Sovereignty and Security Concerns Arising from Cyberspace

Data sovereignty, technological sovereignty, cyber sovereignty and cybersecurity have become important issues that confront states. In the first place, the Internet and data have become indispensable to national governance. Big data is preconditioned as the pool of diverse governmental activities, such as numerous decision-making processes, legislative action, public administration including supervision of financial and banking industry, processing international trade data, monitoring environmental protection, maintaining investment environment, conducting anti-terrorism tasks and narcotics control. In some cases, big data can be used as direct evidence; in other cases, big data may corroborate physical evidence; and it may even serve as the main evidence in administrative, judicial and legislative decision-making processes. As individuals are increasingly active online, some evidence can only be acquired through the Internet. Without the support of the Internet, the effectiveness and efficiency of national governance would suffer significantly.

The characteristics of the Internet and big data also require states to take into account extraterritorial responses and effects, including the principles, rules and standards of the laws of other states, when formulating their own laws and policies. For this reason, even the implementation of a technological method may give rise to disputes over state sovereignty. For example based on the experience of countries such China, South Korea, Singapore and Italy, which used Digital Tracking to help control the spread of COVID-19, Apple and Google Inc. announced a partnership programme to develop an application that would alert mobile phone users who had been in contact with someone diagnosed with COVID-19. Albeit a well-intended act that could help restart the economy after the pandemic, this raised concerns about state sovereignty and privacy. German companies, for instance, called on European developers to collaborate to develop a "European-style" tracking technology rather than to cede basic rights and state sovereignty including cyber sovereignty to Silicon Valley.[13] This illustrates that cyber sovereignty and cybersecurity are already integrated parts of state sovereignty.

Cyber sovereignty and cybersecurity are the two sides of the same coin. Cybersecurity involves areas beyond traditional understanding of sovereignty, making it difficult to precisely define its scope and contents. However, it is generally considered to be concerned, among other things, with the security of electronic

13 "An Open Initiative Led by the European Digital Economy" *HealthyTogether*, available at https://gesund-zusammen.de/en/initiative (visited 11 July 2021). Marko Milanovic and Michael N Schmitt, "Cyber Attacks and Cyber (Mis)Information Operations during a Pandemic" (2020) 11 *Journal of National Security Law & Policy* 247.

processing, storage and transmission of information (whether the information can be transmitted and stored intact without intrusion by unauthorised third parties). In a comprehensive networked society, there is a chance that one's computer may be hacked and email and other information may be stolen, posing a threat to cybersecurity. Data stored by an institution engaged in service industry, product manufacturing or patient care, are private or confidential. Any intrusion into the computers of these institutions would be a violation of privacy or an infringement of confidential information or trade secrets, which would constitute cyber fraud.

The Internet Society once pointed out that "As a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and 'solutions' ranging from the technical to the legislative".[14] In any case, the globalisation of data and the increasing dependence of nations on networks and data have made cybersecurity an issue of grave concern for all nations. Even between allies, nations cannot be completely confident that others will not pose a threat to their cybersecurity.[15]

Cybersecurity may manifest itself differently from national, societal, network company and consumer dimensions. From the national dimension perspective, cybersecurity is primarily concerned with whether national security would be menaced by unauthorised entries into the network. From the social dimension perspective, cybersecurity refers both to the reliability of network and to whether the network content poses a threat to social morals and practices. From the network company dimension, cybersecurity involves the interactions between different protocols, general technical standards as well as routing and addressing systems. From the consumer dimension, security refers to technology, IP rights and other property rights. Entities, enterprises and individuals who are consumers are users of the network and constantly transmit information to the Internet. Consumers instinctively expect national governments and the Internet companies to safeguard the transmitted information from unauthorised access, processing and usage. While a single piece of personal information may have scarce economic value, economic value arises after its clustering by entities such as network companies. Protection

14 See Karen O'Donoghue, "Some Perspectives on Cybersecurity: 2012" *Internet Society* (12 November 2012), available at https://www.internetsociety.org/wp-content/uploads/2017/08/bp-deconstructing-cybersecurity-16nov-update.pdf (visited 11 July 2021). See also Worku Gedefa Urgessa, "Multilateral Cybersecurity Governance: Divergent Conceptualizations and its Origin" (2020) 36 *Computer Law & Security Review* 1, 2.

15 PRISM, a surveillance program conducted by the United States can be a good example. TC Sottek and Janus Kopfstein, "Everything You Need to Know about PRISM" *The Verge* (17 July 2013), available at https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet (visited 11 July 2021). PRISM led to the invalidation of Safe Harbour, the adequacy decision granted by the European Union to the United States. Although the European Union and the United States concluded the Privacy Shield later on, the European Union had been worried about the human rights violation arising from the United States' surveillance; and the Privacy Shield was again declared invalid by the CJEU on 16 July 2020. "FAQs – EU-U.S. Privacy Shield Program Update" *Privacy Shield Framework* (31 March 2021), available at https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update (visited 11 July 2021).

of personal information security is not only an issue of privacy but also a matter of property rights.

The aforementioned discussion shows that the use of cyberspace including the Internet has given rise to many novel concerns, including cybersecurity. Cybersecurity is multidimensional, transnational and international in nature: in particular, as cybersecurity involves sovereignty concerns, it is impossible for any single state to resolve it on its own. What is needed, therefore, is a joint effort of the international community. Global intergovernmental institutions such as the United Nations (UN), regional arrangements and private entities can make a useful contribution to such joint efforts.

IV. Are There International Rules Governing Cyberspace?

A. Efforts made by the UN

The issue of cybersecurity has long been recognised as a serious international concern. As early as 4 January 1998, the United Nations General Assembly (UNGA) adopted Resolution 53/70 calling for the incorporation of cybersecurity into international security. In 1999, the UNGA adopted a resolution declaring that "the dissemination and use of information technologies and means affect the interests of the entire international community", calling for "broad international cooperation" and noting that "technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States".[16] In its report on promoting norms in cyberspace (2013), the Group of Governmental Experts established by the United Nations on the Security of Information and Telecommunications (UN Expert Group)[17] recommended the development of "[v]oluntary, non-binding norms of responsible State behaviour" to "reduce risks to international peace, security and stability".[18] The UN Expert Group proposed 11 norms for consideration by states.[19] These norms include the need for states "to cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security,"[20] to "ensure that their territory is not used

16 UNGA, "Developments in the Field of Information and Telecommunications in the Context of International Security" (4 January 1999) UN Doc A/RES/53/70, 2.

17 The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security was established pursuant to the UNGA Res 66/24. UNGA, "Developments in the Field of Information and Telecommunications in the Context of International Security" (13 December 2011) UN Doc A/RES/66/24, para.4.

18 UNGA, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (22 July 2015) 70th Session (2015) UN Doc A/70/174, para.10.

19 *Ibid*., para.13.

20 *Ibid*., para.13(a).

by non-State actors to commit such acts [internationally wrongful acts]",[21] and to protect "the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression".[22]

Taking into account the distinctiveness of developing countries, the UN Expert Group observed that, while the aforementioned measures "may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity".[23] Clearly, the UN Expert Group's 2013 report emphasised cooperation among members of the international community in enhancing and ensuring the stability and security of ICT. This is an important move taken by the international community, as the ICTs maintain the operation and functions of cyberspace. Yet, according to what norms and standards should such cooperation be carried out? This question was answered in principle by the Group's subsequent report.

In its 2015 report, the UN Expert Group declared that "[i]nternational law, and in particular the UN Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".[24] The reference to the UN Charter indicates that cyberspace governance involves the issue of security for the reason that the fundamental purpose and objective of the UN is to maintain international peace and security. Just as other technologies, cyberspace technology and the ICTs are inherently neutral but may be used for good or evil purposes. Unlike other technologies, ICTs are characterised by global connectivity, technological vulnerability and anonymity in operation. It may, therefore, be easier to employ the ICTs for evil purposes. The UN Expert Group was obviously aware of the potentials of ICTs and indicated that "the malicious use of ICTs can be easily concealed and attribution to a specific perpetrator can be difficult, allowing for increasingly sophisticated exploits by actors who often operate with impunity".[25] In view of the potential threat cyberspace poses to world peace and security, it should be regulated by international law, including the UN Charter.

Unfortunately, as discussed later, it is impossible for the international community to reach any agreement on cyberspace in the near future. For instance the UN Expert Group could not have its report of 2017 adopted due to a disagreement on the determination of countermeasures, self-defence and the application of international humanitarian law. It could be argued that such disagreement is not on whether

21 *Ibid*., para.28(e). In relation to state responsibility for internationally wrongful acts attributable to them, the resolution emphasises that in order for the state to be made responsible, it is sufficient to prove that an ICT activity originates from the territory or the ICT infrastructure of the State. *Ibid*., para.28(f).

22 *Ibid*., para.13(e).

23 *Ibid*., para.14.

24 See UNGA, "Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (24 June 2013) 68th Session (2013) UN Doc A/68/98, para.19.

25 *Ibid*., para.5.

international law is applicable to cyberspace or not, but, rather, on the specific application of individual principles and provisions. Therefore, the response of the international community should not be interpreted as being totally negative. In any event, having realised the potential difficulties in reaching an agreement, the UN Expert Group stressed the importance of municipal law in regulating cyberspace governance and recommended that states should "harmonize legal approaches as appropriate" and consider "how best to cooperate in implementing" norms identified in the document including the part that may be played by private sector and civil society organisations.[26] At the same time, the UN Expert Group openly stated that its recommended norms should be voluntary and non-binding.[27] However, even such non-binding norms contained in the UN Expert Group were not adopted.

The failure of states to reach an agreement on the report of the UN Expert Group does not mean that cyberspace governance is unimportant or not urgent. On the contrary, it shows that cyberspace governance is a matter of great importance, which requires states to proceed with caution. To illustrate this point, it suffices to mention that subsequent to the failure to adopt the UN Expert Group 2017 Report, the General Assembly of the UN adopted two resolutions[28] indicating an emerging international consensus. One of the resolutions was proposed by developed countries including the EU member states, the United States, Canada, Australia and Japan.[29] The other was introduced by China, Russia and some developing countries in Central Asia and Africa.[30]

---

26 *Ibid*., paras.22 and 25.

27 *Ibid*., para.26.

28 For discussions on the two resolutions, see Alex Grigsby, "The United Nations Doubles its Workload on Cyber Norms, and Not Everyone Is Pleased" *Council on Foreign Relations* (15 November 2018), available at https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased (visited 11 July 2021).

29 See UNGA, "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (18 October 2018) 73rd Session (2018) UN Doc A/C.1/73/L.37. This draft resolution was sponsored by Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Malawi, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine, the United Kingdom of Great Britain and Northern Ireland and the United States. The countries proposing this draft resolution formed a new governmental working group (Group of Governmental Experts [GGE]) in 2019. The GGE is not open to other countries, but other UN member states can engage in through informal consultative meetings. See "Group of Governmental Experts" *United Nations Office for Disarmament Affairs*, available at https://www.un.org/disarmament/group-of-governmental-experts/ (visited 11 July 2021). The resolutions proposed by the GGE include two resolutions adopted by the UNGA. UNGA, "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (2 January 2019) UN Doc A/RES/73/266; UNGA "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (18 December 2019) UN Doc A/RES/74/28.

30 See UNGA, "Developments in the Field of Information and Telecommunications in the Context of International Security" (29 October 2018) 73rd Session (2018) UN Doc A/C.1/73/L.27/Rev.1. This revised draft resolution was sponsored by China, Russia, et al. Unlike the GGE, the Open-ended Working Group (OEWG) initiated by the sponsoring countries is open to all countries. The GGE and the OEWG are "independent mechanisms under United Nations auspices". See UNGA, "Developments in

The adoption of these two resolutions suggests that the international community might not have yet reached a consensus on cyberspace governance per se, but a careful analysis of their contents reveals that the two resolutions overlap significantly on many issues of principle. For example both consider that to promote the peaceful use of ICTs and to prevent conflicts arising from their use is "in the interest of all States". Both resolutions draw attention to the need to respect "human rights and fundamental freedoms" in the use of ICTs and to identify mechanisms for the appropriate involvement of the private sector, academia and civil society organisations in cyberspace governance. The applicability and indispensability of "international law, in particular the Charter of the United Nations" to "[t]he maintenance of an open, interoperable, reliable and secure information and communication technology environment" were contained in both resolutions. The statement that "voluntary, non-binding norms, rules or principles of responsible behaviour" for states can reduce risks to international peace, security and stability was included in both resolutions. Most of these contents are taken from the reports of the UN Expert Group. Considering the large number of countries that participated in the two resolutions, which include all the main countries in cyberspace technology and use, the two resolutions evidence some consensus of the international community on the principles and policies of cyberspace governance.

In 2019, the UN General Assembly once again adopted two resolutions—"Advancing Responsible State Behaviour in Cyberspace in the Context of International Security"[31] and "Developments in the Field of Information and Telecommunications in the Context of International Security".[32] These two resolutions essentially reaffirm the principles of the UN Expert Group reports and other resolutions and reiterate the call for states to continue to let the UN Secretary-General know their views and positions on cyberspace security. These two UN resolutions (especially the one sponsored by China, Russia and others) are important in bringing the responsibility of states for internationally wrongful acts into the scope of cyberspace governance. Since the adoption by ILC of the *Draft articles on Responsibility of States for Internationally Wrongful Acts*, the principle of state responsibility has been recognised as part of customary international law. It has been invoked and interpreted by the ICJ, panels and the Appellate Body of the World Trade Organization (WTO) as well as numerous international investment arbitral tribunals. The significance of the UN resolutions is both to reconfirm the applicability of the principles and rules of state responsibility under international law in the context of cyber activities and indirectly recognise the applicability of customary international law to cyberspace.

---

the Field of Information and Telecommunications in the Context of International Security" (12 December 2019) UN Doc A/RES/74/29, para.2.

31 UNGA, "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (12 December 2019) UN Doc A/Res/74/28.

32 UNGA, "Developments in the Field of Information and Telecommunications in the Context of International Security" (n. 30).

B. Efforts by regional arrangements and other bodies

Member states of the Shanghai Cooperation Organisation also proposed their own International Code of Conduct for Information Security (SCO Code of Conduct), which was adopted by the UN General Assembly in 2011. The SCO Code of Conduct emphasises the "need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security," "the need for enhanced coordination and cooperation universally recognized among States in combating the criminal misuse of information technologies", and "the importance of the security, continuity and stability of the Internet, and the need to protect the Internet and other information and communications technology networks from threats and vulnerabilities, and reaffirming the need for a common understanding of the issues of Internet security and for further cooperation at national and international levels".[33]

To realise these purposes, the Code requires the subscribing states to comply with "the UN Charter and universally recognized norms" and not to "use information and communications technologies including networks to carry out hostile activities or acts of aggression, pose threats to international peace and security".[34] Under the SCO Code of Conduct, states are also obliged to "cooperate in combating criminal and terrorist activities which use information and communications technologies including networks, and curbing dissemination of information that incites terrorism, secessionism, extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment".[35]

Efforts to "ensure the supply chain security of information and communications technology products and services" are, among other things, also part of the Code.[36]

In 2015, the UN General Assembly adopted a revised version of the SCO Code of Conduct.[37] The revised Code highlighted the obligation not to use ICTs and ICT network to interfere in the internal affairs of other states[38] and the importance of

33 The preamble of "International Code of Conduct for Information Security". SCO Code of Conduct was adopted by the UNGA on 12 September 2011. UNGA "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" (14 September 2011) 66th Session (2011) UN Doc A/66/359, 3.

34 Ibid., 4, *lit* (b).

35 *Ibid*., *lit* (c).

36 *Ibid*., *lit* (d).

37 UNGA, "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" (13 January 2015) 69th Session (2015) UN Doc A/69/723, para.2. The revised SCO Code of Conduct was incorporated in the Annex.

38 *Ibid*., para.2 (3).

recognising in the online environment the right an individual enjoys in the offline environment.[39] The Code also provides as follows:

> All States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet.[40]

Though the SCO Code of Conduct is a non-legally binding UN document, the detailed rules and principles contained in it, most of which already exist in contemporary international law, are helpful in identifying and determining the rules applicable to cyberspace.

The BRICS countries (Brazil, Russia, India, China and South Africa) also issued a statement supporting the applicability of international law to cyberspace at their 2017 meeting in Xiamen, China.[41] According to the Declaration, cybersecurity and cyberspace governance issues must be handled in accordance with international law. Given the technological strength of the BRICS countries in cyberspace and the breadth and depth of their use of the Internet, this Declaration will have far-reaching implications for the construction of cyberspace governance and, in particular, the application of the principles and rules of international law to cyberspace operation.

In addition to the aforementioned, several sectoral and regional organisations have adopted recommendations on the operation and activities of cyberspace. They include the 1992 Charter of the International Telecommunication Union, the 2001 Budapest Convention on Cybercrime, the Agreement on Information Security adopted by the Shanghai Cooperation Organisation in 2009[42] and the 2014 African Union Convention on Cybersecurity,[43] just to name a few. These international documents mainly provide recommendations and standards for certain aspects of cyber activities. For example the International Telecommunication Union has formulated a Global Cybersecurity Index, which covers cybersecurity measures of its members relating to legal, technical, organisational, capacity-building and international cooperation aspects. To some extent, the Index reflects the position of

39 *Ibid*., para.2 (7).

40 *Ibid*., para.2 (8).

41 See "Full text of BRICS Leaders Xiamen Declaration" *China Daily* (5 September 2017), available at http://www.chinadaily.com.cn/world/2017brics/2017-09/05/content_31575979.htm (visited 11 July 2021).

42 See "Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security" *CIS·Legislation* (16 June 2009), available at https://cis-legislation.com/document.fwx?rgn=28340 (visited 11 July 2021).

43 See African Union, "African Union Convention on Cyber Security and Personal Data Protection" (adopted on 27 June 2014) EX.CL/846 (XXV).

various countries on cyberspace governance.[44] It also demonstrates that the international community is keen on taking specific steps towards cyberspace governance.

Steps on cyberspace governance are also being taken in international trade measures. According to the WTO, regional arrangements that contain provisions on e-commerce and digital trade have increased significantly in recent years.[45] It is important to note that these international documents have the status of international treaties and fall within the scope of international treaty law. They have the binding force on the parties and the effect of confirming the consensus of the international community that cyberspace is governed by international law. The disadvantage of such trade agreements for regulating cyberspace is that they only deal with trade aspects and cannot be expected to cover the whole range of sophisticated issues on the subject matter. Such shortcomings notwithstanding, the regional arrangements and bilateral agreements can fill the vacuum left by the lack of a multilateral agreement.

C. Customary international law could serve as governing rules

It can be concluded that the international community generally accepts that international law, including the UN Charter, applies to cyberspace. As to what specific principles and rules of international law should apply to cyberspace and how they should be applied require further agreement by the states. In absence of such detailed agreements, customary international law rules are applicable. This involves how the customary international rules could be identified and determined to be applicable to cyberspace.

Customary rules of international law have an independent and separate status in international law: a rule of customary law retains such status even if it is stated in identical terms in a treaty. The ICJ said in *Nicaragua case* that the fact that principles of customary law and general international law have been "codified or embodied in multilateral conventions does not mean that they cease to exist and to apply as principles of customary law, even as regards countries that are parties to such conventions".[46] At the merit stage of the same case the ICJ made the following further observation:

> Even if a treaty norm and a customary norm relevant to the present dispute were to have exactly the same content, this would not be a reason for the Court to take the view that the operation of the treaty process must necessarily

44 International Telecommunication Union, "Global Cybersecurity Index 2017" (19 July 2017), available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (visited 11 July 2021).

45 It was reported that more than 60 per cent of the regional trade agreements entered into force between 2014 and 2016 have provisions on e-commerce. See José-Antonio Monteiro and Robert, "Provisions on Electronic Commerce in Regional Trade Agreements (WTO Working Paper ERSD 11/2017)" World Trade Organization Economic Research and Statistics Division (July 2017) 6, available at https://www.wto.org/english/res_e/reser_e/ersd201711_e.pdf (visited 11 July 2021).

46 *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v United States of America*) (Jurisdiction of the Court and Admissibility of the Application) [1984] ICJ Rep 392, [73].

> deprive the customary norm of its separate applicability. Nor can the multilateral treaty reservation be interpreted as meaning that, once applicable to a given dispute, it would exclude the application of any rule of customary international law the content of which was the same as, or analogous to, that of the treaty-law rule which had caused the reservation to become effective.[47]

Hence, whether customary international rules are incorporated into a treaty or not, they are independently and separably applicable to cyberspace.[48]

According to the ILC, to determine the existence of a rule of customary international law, it is necessary to ascertain whether there is "a general practice that is accepted as law (*opinio juris*)".[49] For purposes of determining whether there is a general practice and whether such general practice is accepted as *opinio juris*, "one must look at what States actually do and seek to determine whether they recognize an obligation or a right to act in that way. This methodology, the "two-element approach" underlies the draft conclusions and is widely supported by States, in case law, and in scholarly writings".[50]

In assessing the evidence relating to the identification and determination of rules of customary international law, the ILC Draft Conclusions provide that "regard must be had to the overall context, the nature of the rule and the particular circumstances in which the evidence in question is to be found".[51] The two elements, general practice and *opinio juris*, must be separately ascertained.[52]

In the absence of a treaty or agreement on cyberspace governance, the ILC Draft Conclusions should assist states and other concerned parties (non-governmental organisations, research institutions, computer and Internet companies, etc.) to identify the principles and rules which can be said to have acquired the status of customary international law. For instance Article 51 of the UN Charter identifies the

---

47 *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v United States of America*) (Merits) [1986] ICJ Rep 14, [175].

48 As the ILC observed: "Some important fields of international law are still governed essentially by customary international law, with few if any applicable treaties. Even where there is a treaty in force, the rules of customary international law continue to govern questions not regulated by the treaty and continue to apply in relations with and among non-parties to the treaty". See ILC, "Report of the International Law Commission" UNGAOR 73th Session Supp No. 10 UN Doc A/73/10 (2018), 122 n. 663. This Report contains the draft conclusions on identification of customary international law and commentaries ("ILC Draft Conclusions").

49 *Ibid*., 124, Conclusion 2 of the ILC Draft Conclusions.

50 *Ibid*., 125, Commentary (1) to Conclusion 2. The ILC also stated that the aforementioned view had been confirmed "in the case law of the International Court of Justice". *Ibid*., 123–125 (from Commentary (2) to Conclusion 2).

51 *Ibid*., 126, Paragraph 1 of Conclusion 3 of the ILC Draft Conclusions.

52 Commentary (6) to Conclusion 3 states that "to identify the existence and content of a rule of customary international law each of the two constituent elements must be found to be present" and that "this calls for an assessment of evidence for each element. In other words, while practice and acceptance as law (*opinio juris*) together supply the information necessary for the identification of customary international law, two distinct inquiries are to be carried out. The constituent elements may be intertwined in fact (in the sense that practice may be accompanied by a certain motivation), but each is conceptually distinct for purposes of identifying a rule of customary international law".

individual or collective self-defence as an "inherent right" of states and states that "nothing in the present Charter shall impair" the right, which applies in the event of an armed attack. In supporting the view that the right of self-defence contained in Article 51 of the UN Charter is part of customary international law, the ICJ in *Nicaragua case* observed as follows:

> There is a "natural" or "inherent" right of self-defence, and it is hard to see how this can be other than of a customary nature, even if its present content has been confirmed and influenced by the Charter. Moreover, the Charter, having itself recognized the existence of this right, does not go on to regulate directly al1 aspects of its content. For example, it does not contain any specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law. Moreover, a definition of the "armed attack" which, if found to exist, authorizes the exercise of the "inherent right" of self-defence, is not provided in the Charter, and is not part of treaty law. It cannot therefore be held that Article 51 is a provision which "subsumes and supervenes" customary international law. It rather demonstrates that in the field in question, the importance of which for the present dispute need hardly be stressed, customary international law continues to exist alongside treaty law.[53]

Based on the ILC Draft Conclusions and the ICJ jurisprudence, it is clear that the consensus of the international community, demonstrated through the UN General Assembly resolutions and others, is that international law including the UN Charter and customary international law is applicable to cyberspace. The way forward is to ascertain the applicable customary rules and principles. The sources for identifying and determining such rules and principles should include the ICJ judgments, the WTO panel and Appellate Body reports, investment arbitration panel awards and scholarly writings. Although to list all the customary rules and principles is not possible in an article like this, the most important point is that such rules and principles should include sovereignty, sovereignty security, self-defence, good faith and *pacta sunt servanda*.

In view of the global impact of the cyberspace, the UN Expert Group, UN resolutions and SCO Code of Conduct and others have all emphasised the importance of cooperation among states, international organisations and other bodies and entities in cyberspace operations. Cooperation should therefore be considered as an emerging rule of customary nature. With this approach in identifying and determining the content of the applicable rules and principles of customary international law, and applying such rules and principles, the lack of rules of cyberspace governance will be cured to some extent.

53 See *Military and Paramilitary Activities in and against Nicaragua* (n. 47) [176].

V. Could Regulations by States and Other Bodies Fill the Gap?

A. Regulations by States

In the absence of a multilateral mechanism, regulation at the national level is particularly important. National means of regulating the Internet are quite diverse, ranging from the adoption of specific laws to application of existing laws to the network activities and transactions. Such laws include those on goods and services which apply to e-commerce, digital trade, data transaction, etc. An example is the case involving Microsoft's search warrant, in which the United States District Court (USDC) ruled that Microsoft had a duty under the Stored Communications Act to disclose the contents of its stored emails, including those stored in a database of its wholly owned subsidiary in Ireland.[54] Microsoft objected on the basis that the disclosure of the data stored in the Irish database was extraterritorial, but the USDC held that since Microsoft could remotely control the data stored in Ireland, obliging Microsoft to submit such data did not involve extraterritorial application of the law. Subsequently, the US Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which amended the US Stored Communications Act to add that service providers "shall comply with their obligations under this chapter with respect to the preservation, backup, or disclosure of the contents of communications made over wire or electronically, and records or other information concerning their customers in their custody or control, whether or not such communications, records, or other information are located in the US".[55]

It is not surprising that the United States, being the birthplace of the Internet and the most technologically advanced country, is asserting the extraterritoriality of the US law, only this time it is applying to the Internet what it applies to other areas of law. Admittedly, when all the Internet companies operate in multiple countries, and when all countries regulate the activities of the dot-coms without the necessary coordination between them, national laws of different countries will inevitably conflict with one another.

In terms of conflict of laws, the courts of some countries refuse to apply foreign public law.[56] If such a country considers that the law governing cyberspace is a public law, its courts or data authorities will refuse to apply it in their country. However, this distinction between public and private law, like the distinction between procedural and substantive law, is of little significance in practice. Some commentators believe that "[d]ata protection legislation will typically contain provisions of a public law nature, relating to an authority and its duties and decisions. But the law

54 See *In Re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp*. 15 F Supp 3d 466 (SDNY 2014).

55 The case was eventually appealed to the US Supreme Court. Pending the US Supreme Court's decision, the US Clarifying Lawful Overseas Use of Data Act took effect, and the US Supreme Court terminated the case subsequently. See *United States v Microsoft Corporation* 584 US ____ (2018), 2.

56 See Cedric Ryngaert, *Jurisdiction in International Law* (Oxford: Oxford University Press, 2008) p. 15.

will also often include civil law provisions, typically on liability for data protection violations. The provisions of data protection legislation may therefore have to be qualified as belonging to different areas of law".[57]

This illustrates that even with law enforcement approach, different countries may face different issues. It also shows that it is important to coordinate such cyber-related actions at international level.

B. Regulatory norms proposed by private entities

The lack of agreement at an international level has led other concerned parties to take necessary measures. Preeminent among them is the Global Commission on the Stability of Cyberspace (hereinafter referred to as "the Commission"), founded in 2017[58] and supported by partners, sponsors and supporters, with experts and scholars drawn internationally serving as Commissioners,[59] which has made several normative recommendations relating to the Internet, including "Call to Protect Public Core of the Internet"[60] and "Norm Package Singapore"[61] and briefings addressing the international law issues relating to cyberspace.[62] Representing the results of its work over the past three years, the Commission published its full report entitled "Advancing Cyberstability" in 2019, which proposes a comprehensive Cyberstability Framework with four principles, eight norms of conduct and six recommendations for promoting stability in cyberspace.[63] Although these proposals are not yet universally accepted, given the close relations of the Commission with its member governments and the influence the Commission exerts in

57 See Jon Bing, "Data Protection, Jurisdiction and the Choice of Law" *Privacy Law and Policy Reporter* (1999) 6, available at http://classic.austlii.edu.au/au/journals/PrivLawPRpr/1999/65.html (visited 11 July 2021).

58 Founded by the Government of the Netherlands, The Hague Centre for Strategic Studies and the EastWest Institute. See https://cyberstability.org/news/launch-of-global-commission-on-the-stability-of-cyberspace/

59 Partners include the Government of the Netherlands, Microsoft Corporation, Cyber Agency Singapore, Ministry of Foreign Affairs France and Internet Society. Sponsors include the Federal Department of Foreign Affairs of Switzerland and Ministry of Internal Affairs and Communications of Japan. Supporters include the African Union Commission, Global Forum on Cyber Experience, Google, Tel Aviv University and United Nations Institute for Disarmament. https://cyberstability.org/about/

60 "Call to Protect the Public Core of the Internet" *Global Commission on the Stability of Cyberspace* (November 2017), available at https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf (visited 11 July 2021).

61 "Norm Package Singapore" *Global Commission on the Stability of Cyberspace* (November 2018), available at https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf (visited 11 July 2021).

62 Views of the Commission are often published in the form of Scientific Advisory Panel briefs and memos. See "Briefings from the Research Advisory Group" *Global Commission on the Stability of Cyberspace* (November 2017), available at https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf (visited 11 July 2021).

63 The four principles are specified in Part 5 of the report. The norms and recommendations are incorporated in Parts 6–7. "Advancing Cyberstability" *Global Commission on the Stability of Cyberspace* (November 2019), available at https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf (visited 11 July 2021).

industry, its impact on the direction of norms-making in cyberspace can hardly be underestimated.

Microsoft has also taken the lead in formulating cyberspace-related norms. It drafted the Cybersecurity Tech Accord in 2018, which invited industry participation and pledged commitment to "protecting and empowering civilians online".[64] More than 60 dot-com companies worldwide joined the Accord[65], and many high-tech companies supported it, recognising that cyberspace is public goods of the international community. The Cybersecurity Tech Accord proposes that the operation of network should adhere to four principles. First, participants should protect users from cyberattacks by providing products and services with built-in security and privacy. Second, with respect to cyberattacks, participants should not provide assistance to any government or organisation. Third, participants should provide training to users to use cyber tools and support efforts of civil society, as well as governments and other organisations, in promoting global cybersecurity. Fourth, the participants should enter into formal and informal partnerships to enhance cybersecurity information, including sharing information on cyber threats, patching vulnerabilities and encouraging global information-sharing to protect civilians and help them recover data from cyberattacks.[66] In the same year, 2018, Siemens drafted the Charter of Trust,[67] which was supported and signed by companies from North America, Europe and Japan. As one of its principles, the Charter of Trust recommends the inclusion of cybersecurity in free trade agreements by promoting a multilateral platform for cooperation on rules and standards modelled on the WTO.[68] The Charter of Trust advocates "a level playing field matching the global reach of WTO", partly due to the effectiveness of the WTO rules in facilitating international trade and the interconnection between cyberspace and international trade as well as other economic transactions and exchanges.

In 2015, Microsoft adopted the "Five Principles for Shaping Cybersecurity Norms" (hereinafter referred to as "Microsoft Cyber Norms")[69] which contain norms of conduct to be observed by sovereign states. According to the Microsoft Cyber Norms, the military and intelligence agencies of sovereign nations should exercise restraint in conducting offensive cyber acts to reduce uncertainty for the

64 See "Protecting Users and Customers Everywhere" *Cybersecurity Tech Accord*, available at https://cybertechaccord.org/accord/ (visited 11 July 2021).

65 The agreement was signed by more than 60 high-tech companies shortly after its launch. See "Cybersecurity Tech Accord Expands Rapidly: Announces Partnership with Global Forum on Cyber Expertise (GFCE)" *Tech Accord* (24 September 2018), available at https://cybertechaccord.org/gfce_partnership/ (visited 11 July 2021).

66 See "Protecting Users and Customers Everywhere" (n. 65).

67 See "Charter of Trust: For a Secure Digital World" available at https://www.charteroftrust.com/wp-content/uploads/2021/03/Charter-of-Trust_Principles_EN_2021-02-25.pdf (visited 11 July 2021).

68 Principle 9 is "Regulatory framework" which is to "[P]romote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of the WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs)". *Ibid*., 4.

69 See "Five Principles for Shaping Cybersecurity Norms" *Microsoft*, available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc9 (visited 11 July 2021).

information and communications industry. In terms of defensive measures taken by public institutions and private companies, the Microsoft Cyber Norms advocate cybersecurity risk management through cooperation of all relevant parties by enhancing the ability to defend against and respond to intrusions. Microsoft also asserts in a policy paper that it is the responsibility of network companies to support cyber defence and to avoid cyberattacks.[70]

In many ways, Microsoft has been one of the most influential non-governmental players in norm-making on cyberspace. In addition to the initiatives referred to before, Microsoft launched their "Digital Peace Now"[71] campaign on 28 September 2018. The campaign encourages national leaders to work towards digital peace. Microsoft's work in shaping the norms in cyberspace extends beyond these actions. Microsoft also proposed the drafting of a Digital Geneva Convention[72] and the establishment of an international mechanism for network operations. The Digital Geneva Convention was named after the famed 1949 Geneva Conventions on the laws of war, for example, on protection of civilians and non-combatants in wartime. By the same token, the purpose of the Digital Geneva Convention is to "commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognised that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies".[73]

The international mechanism for network operations aims to establish an intergovernmental or non-governmental organisation to promote the safe operation of the network. Overall, Microsoft's proposed norms on cyberspace governance are mostly recommendatory, made in the hope that states would translate them into mandatory commitments. Towards this end, the Microsoft Network Specification recommends that "[S]tates should have a clear, principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them".[74] This is also the business sector's call for rules to be made by the international community.

The Tallinn Manual on the International Law Applicable to Cyber Warfare ("Tallinn Manual") is another effort in cyberspace rulemaking by a non-state body. Drafted by 19 experts and supported by the Cooperative Cyber Defence Centre of

---

70 "International Cybersecurity Norms" *Microsoft*, available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REY05a (visited 11 July 2021).

71 See "About Us - Digital Peace" *Digital Peace*, available at https://digitalpeacenow.org/about-us/ (visited 11 July 2021).

72 See "Creating a Digital Geneva Convention" *Microsoft*, available at https://news.microsoft.com/cloudforgood/policy/briefing-papers/trusted-cloud/creating-digital-geneva-convention.html (visited 11 July 2021).

73 See "A Digital Rights Approach to the Tech Accord and the Digital Geneva Convention" *access now* (September 2018) 8, available at https://www.accessnow.org/cms/assets/uploads/2018/08/DGC-tech-accord-human-rights.pdf (visited 11 July 2021).

74 See Scott Charney *et al*., "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms" *Microsoft* (June 2016) 7, available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8 (visited 11 July 2021).

Excellence of the North Atlantic Treaty Organization (NATO), the Tallinn Manual was first published in 2013. As its name suggests, the Tallinn Manual focuses on how international law applies to cyberattacks and other cyber operations, which fall under the international law of armed conflict. As the international community is more concerned with how international law applies to the peaceful use of cyberspace, the Tallinn Manual authors published the Tallinn Manual on the International Law Applicable to Cyber Operations, also known as the Tallinn Manual Version 2.0, in 2017,[75] which contains 154 rules covering both peaceful use and non-peaceful use of cyberspace.

On the whole, the rules proposed in Tallinn Manual reflect the generally accepted principles of international law such as sovereignty, sovereign immunity, territorial and personal jurisdiction of states and responsibility of states for internationally wrongful acts. The manual also contains novel rules including due diligence, cooperation in law enforcement and responsibility of international organisations. Those relating to the traditional international law rules overlap, to some extent, with the recommendations of the UN Expert Group and UN General Assembly resolutions discussed before. They, therefore, have the effect of supplementing and redefining the customary rules of international law. Even the novel rules that the Tallinn Manual Version 2.0 proposed could have a positive effect on rulemaking to govern cyberspace and cyber operations. For instance Rule 11 entitled "Extraterritorial enforcement jurisdiction" provides as follows:

> A State may only exercise extraterritorial enforcement jurisdiction in relation to persons, objects, and cyber activities on the basis of: (a) a specific allocation of authority under international law; or (b) valid consent by a foreign government to exercise jurisdiction on its territory.[76]

This implicitly recognises the customary international law principle of sovereign equality and non-interference of internal affairs of states. It is hard to ignore the positive effect of even the controversial Rule 7 (Compliance with the due diligence principle),[77] which "requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States". Needless to say that it is questionable whether there is such a principle of due diligence on the part of states in contemporary international law. Yet, the raising of the question itself is important for the international community.

Authors of the Tallinn Manual have always claimed that their work was private in nature. In view of the relationship between the Tallinn Manual and NATO, some doubt whether it only represents the personal views of the authors and not those of

75 See Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

76 *Ibid*., 66.

77 *Ibid*., 55.

NATO. Given the relationship among the Tallinn Manual project, its authors and NATO, it is unlikely that some statements by the authors could dispel the perception that the Tallinn Manual reflects some views of the NATO too.

C. The potential effects of the norms recommended by private entities

Rules adopted by private companies and non-governmental entities do not bind states. However, in a highly information-based world, the actions of non-governmental entities and private companies may have an important impact on the international level and indirectly influence international norms-making in the relevant areas and become mutually reinforcing with the actions of state.

The spill over effects of rules and norms formulated by private companies and others in relation to cyberspace including digital trade should not be overlooked, as sometimes such norms are made primarily relating to actions of national governments. The rules and norms proposed by these institutions and entities, with the backing of some states, are actually conducive to rule-making for cyberspace governance. These rules are particularly important when negotiations at the international level on the formation of an international cyberspace order make no noticeable progress. Yet, the enthusiasm of non-governmental entities in formulating rules on cyberspace cannot replace or substitute the part that states must play.

It must also be borne in mind that no matter how rapidly cyberspace develops, and no matter how the rules and norms of cyberspace governance are formulated by non-governmental institutions and private entities, they must ultimately be endorsed by sovereign states before they can become binding on states, philosophical arguments on subjects and objects of international law notwithstanding.[78] There is no substitute for the status and role of sovereign states in making rules for cyberspace governance.

VI. Prospects of Cyberspace Governance

A. Effects of international law on cyberspace

One of the functions of law is to distinguish between legal and illegal acts. The role of international law is to set standards for the conduct of states and other actors. As such, the legality of a sovereign state's conduct depends on the specification

78 The former ICJ Judge Higgins, however, considers this traditional view not to be helpful and argues that "international law is not to be understood as a set of 'rules'. First of all, international law is not only 'rules'; moreover, its norms are not fixed indefinitely and are thus wholly responsive to the needs of the system. Further, the positivist definition assumes that some specific rule is required 'permitting' the individual to be a 'subject' of international law. Finally, the whole notion of 'subjects' and 'objects' has no credible reality, and, in my view, no functional Purpose". See Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Clarendon Press, 1995) p. 49.

and application of international treaties, agreements and customary international law. This includes the application of existing rules to newly emerging areas such as cyberspace. Private versions of norms, standards and recommendations adopted by cyber corporations, institutions, non-governmental organisations and others on cyberspace governance have a positive effect on building an international legal order. Nonetheless, the endorsement of sovereign states is a necessary condition for these norms to be elevated to the status of international law. As the construction of an international cyberspace legal order involves the fundamental interests of sovereign states, it is highly unlikely that a global multilateral agreement can be reached in the short term. All the while, humanity is becoming increasingly dependent on cyberspace. Nonetheless, the development of laws and rules always lags behind the development of things they are intended to regulate, making it difficult to keep pace with social and technological progress. This is particularly true of international rules on new technologies such as cyberspace.

In these circumstances, possible options for states are to confirm the applicability of existing principles and rules of international law through bilateral and regional agreements and to develop new rules to regulate the cyberspace. In this regard, it is worth learning from the experience of the WTO. In the first place, though the WTO is a predominantly multilateral mechanism, it is supplemented and complemented by bilateral and regional arrangements. Second, WTO is innovative in implementing its rules by applying the principle of technology neutrality.[79] States must adopt the same approach in the area of cyberspace.

B. State sovereignty and cooperation as essential rules governing cyberspace

As mentioned before, there is a general consensus that international law, including the Charter of the United Nations, is applicable to cyberspace. The subsequent question is which principles and rules of international law apply to users. Contemporary international law is gradually formed based on the Peace of Westphalia and its resulting system,[80] whose principles include sovereign equality, non-interference in internal affairs, *pacta sunt servanda* and peaceful settlement of disputes.[81] The

79 The WTO's panels and Appellate Body have never openly admitted that they would apply the principle of technological neutrality, though in practice they have. At the same time, in its Work Programme on Electronic Commerce, a Progress Report to the General Council, the Council for Trade in Services stated that "[i]t was also the general view that the GATS is technologically neutral in the sense that it does not contain any provisions that distinguish between the different technological means through which a service may be supplied". See World Trade Organization, "Work Programme on Electronic Commerce - Progress Report to the General Council" (27 July 1999) S/L/74, para.4, available at https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/S/L/74.pdf&Open=True (visited 11 July 2021).

80 For discussions on the Westphalian system, see Guiguo Wang, "The Post-COVID-19 International Order and China's Role" (2020) 4 *China Law Review* 1, 1–4.

81 The UN Charter provides in Article 33 that "[t]he parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution

Westphalian model of international law resulted from economic interdependence of all countries, which initially reflected the culture, traditions, customs, values, laws and religions of the Western countries. After centuries of evolution, international law combined features of Eastern and Western cultures and has become an international code of conduct recognised by the international community. State sovereignty is the overriding principle of the contemporary international law. It is only by recognising equality of sovereign states that nations may effectively cooperate and interact and achieve international peace. Therefore, the fundamental principles of international law of cyberspace must be principle of sovereignty and the principle of cooperation.

The principle of sovereignty emphasises the jurisdiction of sovereign states in cyberspace, including the operation of the Internet, the storage and movement of data and the modes and standards of operation of network platforms. The principle of cooperation is based on the general environment of economic globalisation and reflects the necessity and reality of extensive cooperation among states at the economic level, including in cyberspace. Necessity refers to the fact that in the context of globalisation, where the interdependence of states is increasing rapidly in many fields and at many levels, no state can develop independently, and cooperation is the only way to benefit each state. Reality refers to the fact that only by acknowledging the realities of the world and taking measures in line with the world trends can cyberspace be effectively managed.

C. Formulation of particular customary rules to govern cyberspace

In applying the aforementioned international law principles and others, special attention should be paid to the formation and emergence of new and particular customary rules of international law. This is not easy as the "formation of a customary law in a given society, be it municipal or international, is a complex psychological and sociological process, and therefore, it is not an easy matter to decide".[82] In any event, Judge Tanaka of the ICJ considered that "the process of generation of a customary law is relative in its manner according to the different fields of law", and that "it can be recognized that the speedy tempo of present international life promoted by highly developed communication and transportation had minimized the importance of the time factor and has made possible the acceleration of the

by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice".

82 Judge Tanaka also said: "To decide whether these two factors in the formative process of a customary law exist or not, is a delicate and difficult matter. The repetition of the number of examples of State practice, the duration of time required for the generation of customary law cannot be mathematically and uniformly decided". Dissenting Opinion of Judge Tanaka, *North Sea Continental Shelf* (*Federal Republic of Germany v Denmark /Netherlands*) (Dissenting Opinion of Judge Tanaka), [1969] ICJ Rep 3, 175.

formation of customary international law. What required a hundred years in former days now may require less than ten years".[83]

Differing slightly from Judge Tanaka, the majority of the ICJ held as follows:

> Although the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law on the basis of what was originally a purely conventional rule, an indispensable requirement would be that within the period in question, short though it might be, State practice, including that of States whose interests are specially affected, should have been both extensive and virtually uniform in the sense of the provision invoked; and should moreover have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved.[84]

The ICJ judgment, however, does not exclude the possibility of forming a customary international law rule in a relatively short period of time, provided that there is proof of both usage and *opinio juris* of those affected by the rule. In this regard, the actions and omissions of states must be carefully analysed. In the view of the ICJ in the *Nicaragua case*: "[i]f a State acts in a way *prima facie* incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State's conduct is in fact justifiable on that basis, the significance of that attitude is to confirm rather than to weaken the rule".[85] It is therefore quite possible that even an apparent reaction to a given rule may constitute recognition of the same.

In addition to the general customary international law rules, there can be special or particular customary rules and principles. This is confirmed by the ILC Draft Conclusions which provide that "[a] rule of particular customary international law, whether regional, local or other, is a rule of customary international law that applies only among a limited number of States".[86] This is also confirmed by the ICJ's practice that such particular rules may be formed among a group of countries within a region or even two states.[87] Based on the logic of the ICJ practice and ILC Draft Conclusions, it could be argued that some special or particular rules of customary

83 *Ibid*., 177.

84 *North Sea Continental Shelf* (*Federal Republic of Germany v Denmark /Netherlands*), [1969] ICJ Rep 3 [74].

85 See *Military and Paramilitary Activities in and against Nicaragua* (n. 47) [186].

86 "Report of the International Law Commission" (n. 48), Conclusion 16, 154–156.

87 For instance in the *Colombian-Peruvian Asylum Case*, the ICJ said that there could be customary rules "peculiar to Latin-American States". See *Asylum* (*Colombia v Peru*), [1950] ICJ Rep 266, 276; and in *Case concerning Right of Passage over Indian Territory*, the Court ruled that "it is difficult to see why the number of States between which a local custom may be established on the basis of long practice must necessarily be larger than two. The Court sees no reason why long continued practice between two States accepted by them as regulating their relations should not form the basis of mutual rights and obligations between the two States". See *Right of Passage over Indian Territory* (*Portugal v India*) (Merits) [1960] ICJ Rep 6, 39.

international law can be created among those countries which are major cyberspace technology owners and users. They may or may not need to be geographically connected in order to form a special group. By recognising the special status of such countries, they, as a group or sub-group, may formulate their own customary rules on cyberspace through usage and recognising it as an obligation, that is *opinio juris*. Such customary rules among small groups of countries will help create general customary rules of international law. In addition, as discussed earlier, cyberspace companies and entities have adopted cyberspace norms themselves. Though such norms do not have binding force on the states, they should be able to help identify and determine the existence of customary rules on cyberspace governance.

D. Protection of privacy and personal and social data to be emphasised in the future

Regarding the future direction of cyberspace governance, one must be aware that with cyberspace technologies and services rapidly increasing, privacy and protection of personal data and social data have become an important issue. Usually, when people use the Internet, they are required to provide personal and other information, that is data. Such data by themselves may be of little value. Once an Internet company collects such data from many individuals and put them together, it may use such collection of data for commercial purposes or sell the same to other companies which will use them for their own purposes. This gives rise to the need to protecting such data as it involves privacy, IP rights and other economic interests. In comparison, business-related data such as trademarks and trade secrets are protected by company law and IP law. Yet, except in the EU, there is no existing multilateral mechanism for personal data protection.

The EU regime is the most comprehensive on data protection regulation. The EU regime, with EU General Data Protection Regulation as its core, requires all countries cooperating with it to provide the same level of protection for data and provides a template for data protection legislation in other countries. In practice, the EU has also shown great commitment to enforcing data protection rules. On 16 July 2020, for instance the European Court of Justice (ECJ) ruled that the EU–US data transfer agreement, known as the Privacy Shield Framework, was invalid because the agreement failed to protect EU nationals from US surveillance.[88] The effect of the ECJ decision is that under the agreement, US companies cannot continue to transfer data on EU nationals to the United States. The Privacy Shield Agreement was reached between the EU and the United States in 2016 to replace the Safe Harbour Agreement, which was ruled invalid in 2015. The purpose of the

88 For a discussion of this decision, see Marie McGinley and Neasa Ní Ghráda, "Schrems II Judgement: EU:US Privacy Shield Framework for Personal Data Transfers is Invalidated; Standard Contractual Clauses Need Re-assessment" *Eversheds Sutherland* (20 July 2020), available at https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/global/ireland/schrems-ii-judgement-170720 (visited 11 July 2021).

Privacy Shield Agreement is to ensure that Europeans are afforded privacy protection when their personal data is transferred to the United States for business purposes. According to statistics, more than 5,000 US businesses have signed the Privacy Shield contract, including social media, banks, law firms and corporations. The ECJ held that the Privacy Shield Agreement's restrictions on US access to data failed to meet the EU standards: for instance because there is no provision for nationals of EU member states to challenge a decision to put them under surveillance by the US government. The Court of Justice of the European Union (CJEU) also ruled that companies may continue to use Standard Contractual Clauses (SCC) to transfer data. The SCC needs to be signed by the companies concerned on a case-by-case basis to ensure that the processing of data transferred to the United States complies with the EU General Data Protection Regulation. The EU and the United States are key players in the governance of digital technology and cyberspace, and their domestic laws are the most influential. The differences in the relevant law between the EU and the United States reflect the challenges of cyberspace governance in the international community, illustrate the urgency of building a regime that is recognised by the states and suggest a direction for thinking about how to build a multilateral regime.

Last but not the least, Lao Tzu once said that "[A]ction should be taken before a thing has made its appearance; order should be secured before disorder has begun".[89] Cyberspace technologies continue to develop rapidly, and the international community cannot afford to waste any more time in establishing an international cyberspace legal order—it is time to consummate it.

89 Lao Tzu, *Tao Te Ching* (translated by Man-Ho Kwok, Martin Palmer and Jay Ramsay, Dorset: Element,1993) Ch. 64.