ISSUE: 2023, No. 03

AVI POLICY BRIEF

Cambodia | 13 April 2023

Making of International Cyberspace Law

TEAN Samnang *

Executive Summary

- Due to the pervasive reliance that state and non-state actors have on cyberspace and the increasing peril the domain poses, powerful states have pushed for the security of this realm. However, no uniform set of norms or laws governing cyberspace currently exists.
- Overall, the attempts of multiple international communities to establish suitable international institutions and laws on cyberspace have been unsuccessful. Consequently, cyberspace governance has been delegated to individual states for determination.
- The development at hand has impeded progress towards establishing a suitable international legal framework for cyberspace, despite genuine and earnest efforts to do so. The efforts to establish regulations for the cyber realm have been persistently impeded or have encountered insufficient backing from some entities.

សេចក្តីសង្ខេបអត្ថបទ

- ដោយសារការពឹងផ្អែកយ៉ាងទូលំទូលាយ ដែលតួអង្គរដ្ឋ និងតួអង្គមិនមែនរដ្ឋមានមកលើលំហអ៊ីនធឺណិត និងការកើនឡើងនៃគ្រោះថ្នាក់កើតចេញពីលំហរនេះ រដ្ឋដែលមានឥទ្ធិពលបានជម្រុញអោយមានការធានាសន្តិសុខនៃប្រព័ន្ធនេះ។ ទោះជាយ៉ាងនេះក្តី មកទល់បច្ចុប្បន្ននេះ មិនទាន់មានច្បាប់កំណត់ ឬនិយាមគ្រប់គ្រងជាអន្តរជាតិសម្រាប់លំហរនេះនៅឡើយទេ។
- ជារួម ការប៉ុនប៉ងរបស់សហគមន៍អន្តរជាតិជាច្រើនដើម្បីបង្កើតស្ថាប័នអន្តរជាតិ និងច្បាប់អន្តរជាតិដើម្បីគ្រប់គ្រងលំហរអ៊ីនធឺណិត មិនទាន់ទទួលបានជោគជ័យទេ។ អាស្រ័យហេតុនេះ អភិបាលកិច្ចនៃប្រព័ន្ធអ៊ីនធឺណិត ត្រូវបានផ្ទេរទៅឱ្យរដ្ឋនីមួយៗដើម្បីធ្វើការគ្រប់គ្រង។
- ការអភិវឌ្ឍនេះមានការរារាំងវឌ្ឍនភាពនៃការបង្កើតបទដ្ឋានគតិយុត្តជាអន្តរជាតិដែលសមស្របមួយ បើទោះជាមានការខិតខំប្រឹងប្រែងពិតប្រាកដ និងដោយស្មោះក្នុងការសម្រេចនៅគោលដៅនេះក៏ដោយ។ ការខិតខំប្រឹងប្រែងដើម្បីបង្កើតបទប្បញ្ញត្តិសម្រាប់ប្រព័ន្ធអ៊ីនធឺណិតនេះ ត្រូវបានរារាំងជាប្រចាំ ឬទទួលបានការគាំទ្រមិនគ្រប់គ្រាន់ពីបណ្តាស្ថាប័នអន្តរជាតិមួយចំនួន។

* **TEAN Samnang** is a PhD Candidate at the School of International Law at the Southwest University of Political Science and Law, China.

Introduction

Technology has altered the lives of individuals. It advances a new way of life moulded by the COVID-19 pandemic and provides new possibilities for humankind to explore and utilise cyberspace and the digital world. To put this into perspective, the number of people who use the internet increased substantially from 4.1 billion people in 2019 to 4.9 billion in 2021 (ITU 2021). This dramatic increase has created an environment for a quick evolution of digitalisation for people's day-to-day activities, as well as for government and commercial purposes. In other words, the world is undergoing the Fourth Industrial Revolution (4IR), driven by technological advancements and the internet (Ali et al. 2022). Against this backdrop, the development of cyberspace, as a result of 4IR, has undergone a transformation, expanding a new battlefield in international politics drawn from the experiences of competing interests in land, air, sea, and outer space domains (McGuffin and Mitchell 2014).

On the one hand, this new cyberspace appears to be a blessing. On the other hand, it causes concern. Heated discussions are on the rise among policymakers, lawmakers, researchers, academics, and the general public (Phau et al. 2014). This growing attention is due to cyberspace's borderless and virtual characteristics, which generate misunderstanding and disparity in comprehension among the parties involved (Heller 2021).

Furthermore, because of its inherent fuzziness, cyberspace is riddled with legal vulnerabilities that can be exploited by various players beyond states to conduct illegal activities directed at individuals or beyond (Adamson 2020). Due to the threats posed by this emerging domain, various players have moved independently to build up their defensive capacity (Bund and Pawlak 2017). To deal with such unpredictability and establish an orderly international society, the fundamental principle of the rule of law has been extolled numerous times. This article examines the existing international laws on cyberspace and the issues concerning applying the laws universally.

Some Attempts to Create Cyberspace Law

Regulating cyberspace under a single, consistent set of rules or laws has not yet been established (Xinmin 2016). The securitisation of cyberspace has emerged as a topic of discussion on several international platforms, led by powerful states, due to the widespread dependence on this new domain and the heightened danger it poses (Domingo 2016). Since there is no universally accepted legal framework governing cyberspace, it is vital to understand the efforts being made by the international community to establish some forms of governance over this domain.

It is clear that the United Nations (UN) plays a pivotal part in any conversation involving the concept of global standards or laws and international concerns regarding peace and security. The UN has previously discussed both the rules and realm of cyberspace. Russia first brought this matter to the attention of the UN General Assembly in 1998 when it submitted a draft resolution titled "Developments in the Field of Information and Telecommunications in the Context of International Security" (Raymond 2021). Because of this proposal, a specialised body known as the United Nations Groups of Governmental Experts (UNGGE) was established to investigate the potential dangers posed by cyberspace and devise a legislative framework to mitigate the risk and keep it under control (Douzet, Géry and Delerue 2022). However, the group included only 15 to 25 UN member states, which were selected based on their geographical distribution, and the decision was made through consensus (Painter 2021).

The UNGGE has had success on two separate occasions. First, in 2013, it adopted 11 voluntary norms for responsible state behaviours in cyberspace to support the peace and security principle of the UN. Second, in 2015, it confirmed that the UN Charter and the other principles of international law applicable to cyberspace (Akande et al. 2022). Both of these accomplishments were noteworthy for the group.

However, despite significant progress, the group could not reach a consensus in 2017 regarding the publication of their recommendations or reports (Painter 2021). This disagreement involved the applicability of the existing international law on the use of force and the law of armed conflicts, which garnered diverse opinions among states (Douzet et al. 2022). This divergence demonstrates that there is no unified legal interpretation of the rules that apply to cyberspace. The idea that the existing international law and the UN Charter apply to the real world is just as nebulous as it demonstrates (Xinmin 2016).

In 2018, there was a further divide in the effort to establish a legal procedure for this domain because two patterns confronted one another. In contrast to the current UNGGE, the UN Open-Ended Working Group (OEWG) was created and tasked with focusing on technology and norm-making (Ruhl et al. 2020). While the UNGGE is an American invention, the OEWG is spearheaded by Russia (Ruhl et al. 2020). Although the subject matter has not changed, the OEWG has broadened its scope to include all UN members (Douzet et al. 2022). Generally speaking, these two platforms have not yet produced any legally enforceable standards or rules as international cyberspace continues to be devoid of legislation (Painter 2021).

The International Telecommunication Union (ITU), the UN's specialised agency on matters related to information and telecommunication technology (ICT), should also be highlighted. In 2012, an attempt was made to amend the ITU's International Telecommunication Regulations (ITRs), a binding treaty for the member states (Fidler 2013). The role of the 1988 ITRs was to oversee communication and network of telephones, radio, and other telecommunication instruments; however, the 1988 ITRs were not scoped to cover the internet (Bennett 2012). Therefore, the ITU's 2012 amendment was supposed to be expanded to cover cyberspace and govern the cyberspace network and communication to improve online safety (Fidler 2013). However, the suggestion was rejected by some Western states because they believed it would harm internet freedom, while the rest were concerned about their national security (Housen-Couriel 2014). Hence, the rules and conventions governing cyberspace continue to be disparate and will unlikely become consistent anytime soon.

Outside of the UN, various efforts by international community actors to find appropriate international organisations and legislation for cyberspace have not produced desirable results yet. However, those initiatives have significant value and potential to serve as a foundational component of a future global convention for cyberspace. For example, the Council of Europe initiated the Convention on Cybercrime, which went into effect in 2004 (Clough 2014). The convention has one main purpose: to lay the groundwork for legal action and the battle against illegal activities and other types of online criminal behaviours (Clough 2014). The convention has been signed by more than 60 states, of which approximately one-third are located outside of Europe. However, since the convention was initiated in Europe, states like Russia, China, and India did not embrace it (Radoniewicz 2022). Moreover, some believe that the convention represents only European views, not those of the rest of the world (Baron 2002).

In a similar vein, the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), a collection of NATO specialists, began to create legal jurisprudence in 2009 for the

legal interpretation of cyberwarfare by representing the existing law of war (Liu, 2017). This was done to ensure that cyberwarfare was not illegal and contend that the law of war, as it stands today, should be applied to technology (Jensen 2017). The scholarly jurisprudent's handbook was non-binding; however, it has been supported by most Western nations, which tend to influence the global legal process (Chircop 2019). On the other hand, NATO CCD COE has been rejected by countries like Russia and China (Henriksen 2019).

Therefore, unsurprisingly, after about 25 years on the international agenda, essential legal concepts governing cyberspace have not been established yet. As a result, the administration of cyberspace is left for individual states to determine.

Geopolitics of Cyberspace Law

It is vital to note that politics and law can be difficult to distinguish. As illustrated earlier, different attempts to establish standards for cyberspace have been consistently thwarted or have received no support from various organisations. The competition demonstrates that the world's most powerful countries, such as the United States, Russia, and China, are concerned about their hegemonic position in this domain. It is common knowledge that the US is home to both the Internet Corporation for Assigned Names and Numbers (ICANN), an organisation responsible for assigning domain names and allocating web space to websites around the world, as well as the National Security Agency (NSA), which has demonstrated its powerful ability to carry out online surveillances that are deemed as a threat to China and Russia (Liaropoulos 2017).

Meanwhile, Russia and China possess offensive cyber capabilities, which allow them to pose a danger not only to the US but also to other countries by conducting surveillance and prying into the critical infrastructure of those countries (Rugge 2018). Therefore, challenging the status quo, particularly the legal interpretation concerning cyberspace, would hinder the interests of different states.

In addition, ideological disagreements are another factor contributing to the increasing fragmentation of the internet. While the US and its allies have advocated strongly for the freedom of cyberspace, China and Russia have favoured state sovereignty in the management of cyberspace (Shen 2016). The US adopts terms such as "cybersecurity" to refer to only the administration of cyberspace infrastructure. In contrast, China and Russia use the term "Information and Communication Technology Security" to include both the infrastructure and the information movements in the domain susceptible to state control (Lumiste 2022). As a result, a sincere endeavour to establish an appropriate body of international law on cyberspace remains hindered by these divisions among major powers, which are also influential norm-setters.

Conclusion

An international law governing cyberspace has not yet been established due to the absence of a common ground and a shared understanding, driven by the competition between states. Although attempts have been made to regulate this domain, the results have been inconsistent and patchy. However, it is essential to remember that in the absence of appropriate cyberspace governance, disorder and new problems will emerge. Therefore, existing issues should not be allowed to persist any longer. Considering this conundrum, governments around the globe should take into consideration the following recommendations:

- First, states should collaborate in good faith to find solutions to cyberspace. Discussions should take place on platforms that allow inclusive participation from all stakeholders, specifically small and less influential states. In addition, inclusiveness can guarantee transparency and straightforwardly decrease mistrust. The ITU is a viable platform for such an arrangement.
- Second, the prospect of collaboration among states should always be open to consideration. As already mentioned, cyberspace is rife with risks and uncertainties. Consequently, states with fewer resources may be more susceptible to the ramifications of such occurrences. If the superpowers act according to their interests and limit the interests of small states, primarily through establishing a norm or rules unilaterally to impose on the outsider, they will create a legalised hegemony in which a compromise for a fair and just governance system of cyberspace cannot be reached.
- In conclusion, scepticism and improper interpretation could be the sources of the disagreement. Consequently, powerful states ought to search for an objective party or an experienced organisation that can manage the conflicts or serve as an arbitrator and act as a neutral party to mediate existing contentions. Without a legislative committee, differences will continue, and states may be forced to approach the problems independently rather than collectively.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

References

Adamson, Liisi. 2020. "International Law and International Cyber Norms A Continuum?" In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders Bibi van den Berg. New York: Rowman & Littlefield.

Akande, D, A Coco, and Talita de Souza Dias. 2022. "Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies." *International Law Studies* 99 (4), 5-39.

Ali, Norhidayah, Zuraidah Mohamed Isa, Suhaida Abu Bakar, Fathiyah Ahmad Ahmad Jali, and Sarah Shaharruddin. 2022. "Industrial Revolution (IR) 4.0: Opportunities and Challenges in Online Business." *Proceedings* 82 (85): 1–9.

Baron, Ryan M F. 2002. "A Critique of the International Cybercrime Treaty." *Commlaw Conspectus* 10: 263–78.

Bennett, B Y Richard. 2012. "The Gathering Storm : WCIT and the Global Regulation of the Internet." *The Information Technology & Innovation Foundation*, no. November: 1–19.

Bund, J, and P Pawlak. 2017. "Minilateralism and Norms in Cyberspace." *European Institute for Security Studies*, no. September: 1–2.

Chircop, Luke. 2019. "Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0." *Melbourne Journal of International Law* 20 (2): 349–377.

Clough, Jonathan. 2014. "A World of Difference : The Budapest Convention on Cybercrime and the Challenges of Harmonisation." *Monash University Law Review* 40 (3): 698–736.

Domingo, Francis C. 2016. "Conquering a New Domain: Explaining Great Power Competition in Cyberspace." *Comparative Strategy* 35 (2): 154–68.

Douzet, Frédérick, Aude Géry, and François Delerue. 2022. "Building Cyber Peace While Preparing for Cyber War." *Cyber Peace* 27: 170–92.

Fidler, David P. 2013. "Final Acts of the World Conference on International Telecommunications." *International Legal Materials* 52 (3): 843–60.

Heller, Kevin Jon. 2021. "In Defense of Pure Sovereignty in Cyberspace." *International Law Studies* 97: 1431–99.

Henriksen, Anders. 2019. "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace." *Journal of Cybersecurity* 1 (5), 1–9.

Housen-Couriel, Deborah. 2014. "The 'Dubai Clash' at WCIT-12: Freedom of Information, Access Rights, and Cyber Security." Institute for National Security Studies.

International Telecommunication Union (ITU). 2021. "Measuring Digital Development: Facts and Figures." *International Telecommunication Union*, 1–31.

Jensen, Eric Talbot. 2017. "The Tallinn Manual 2.0: Highlights and Insights." *Georgetown Journal of International Law* 48: 736–77.

Liaropoulos, Andrew N. 2017. "Cyberspace Governance and State Sovereignty." In *Democracy and an Open-Economy World Order*, edited by George C. Bitros, Nicholas C. Kyriazis, 25–35. Springer Cham.

Liu, Ian Yuying. 2017. "The Due Diligence Doctrine under Tallinn Manual 2.0." *Computer Law and Security Review* 33 (3): 390–95.

Lumiste, Liina. 2022. "Russian Approaches to Regulating Use of Force in Cyberspace." *Baltic Yearbook of International Law* 20 (1): 11–132.

Maurer, Tim. 2020. "A Dose of Realism: The Contestation and Politics of Cyber Norms." *Hague Journal on the Rule of Law* 12 (2): 283–305.

McGuffin, Chris, and Paul Mitchell. 2014. "On Domains: Cyber and the Practice of Warfare." *International Journal: Canada's Journal of Global Policy Analysis* 69 (3): 394–412.

Painter, Christopher. 2021. "The United Nations' Cyberstability Processes: Surprising Progress but Much Left to Do." *Journal of Cyber Policy* 6 (3): 271–76.

Phau, Ian, Min Teah, and Michael Lwin. 2014. "Pirating Pirates of the Caribbean: The Curse of Cyberspace." *Journal of Marketing Management* 30 (3–4): 312–33.

Radoniewicz, Filip. 2022. *International Regulations of Cybersecurity*. *Cybersecurity in Poland*. https://doi.org/10.1007/978-3-030-7855.

Raymond, Mark. 2021. "Social Practices of Rule-Making for International Law in the Cyber Domain." *Journal of Global Security Studies* 6 (2), 1-24.

Rugge, Fabio. 2018. "An 'Axis' Reloaded ?" In *Confronting An "Axis of Cyber"?: China, Iran, North Korea, Russia in Cyberspace,* edited by Fabio Rugge, 13–38. Milano-Italy: Ledizioni LediPublishing.

Ruhl, Christian, Duncan Hollis, Wyatt Hoffman, and Tim Maurer. 2020. "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads." Carnegie Endowment for International Peace.

Shen, Yi. 2016. "Cyber Sovereignty and the Governance of Global Cyberspace." *Chinese Political Science Review* 1 (1): 81–93.

Xinmin, Ma. 2016. "Key Issues and Future Development of International Cyberspace Law." *China Quarterly of International Strategic Studies* 2 (1): 119–33.