sciendo
Vietnamese Journal of Legal Sciences, Vol. 09, No. 02, 2023, pp. 01-26 DOI: 10.2478/vjls-2023-0007

INTERNATIONAL LAW PROTECTION IN CYBERSPACE AGAINST RANSOMWARE AND EXPERIENCE OF VIETNAM

MAC TRANG ANH
AstraIA Gear, France
Email: tranganh.mac@astraiagear.com

Abstract

Amongst various cyberattacks, ransomware adversely affects the business operation as the malware locks the computer or data, and menaces to keep it locked unless a ransom is transferred. In a young tech market like Vietnam, cyberattacks, including ransomware, cause serious concerns for State and non-State actors. They can take place anywhere since cyberspace has no physical border to hold them back. This raises a query about the application of international law in cyberspace, especially when the ransomware hits non-State actors. In such cases, the sovereignty principle, having a significant relation with the jurisdiction, underpins the intervention of national authorities and regulation of ransomware. Vietnam's government has intensified their efforts to stop the cyberattacks by cooperating with other countries and establishing a legal framework based on the international law principle.

Keywords: *international law, sovereignty, jurisdiction, cyberspace, ransomware*
Received: 4 December 2023/Revised: 18 December 2023/Accepted: 19 December 2023

In his declaration in 1996, John P. Barlow developed the independence of cyberspace and rejected the State's sovereignty and legal conceptions in the network[1] in response to the adoption of the Telecommunications Act of 1996 in the United States (the US), one of the first milestones of legislation governing the Internet.[2] Cyberspace is a term which was first introduced by William Gibson in 1984 as the space "where human interaction occurs over computer networks, through email, games or simulations".[3] According to United States law, it is defined as "[…] the interdependent network of information technology infrastructures; and […] includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[4] Vietnamese laws determine cyberspace as "the connected network of information technology [IT] infrastructure comprising telecom networks, the Internet, computer networks, information systems, information processing and control systems, and databases, where people perform social acts without being limited by space and time".[5] Today, it is undeniable that these arguments of J. P. Barlow did not become

1 Barlow J. P. (1996), 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/cyberspace-independence [accessed 29 November 2023].
2 Ehrlich E. (2014), 'A Brief history of Internet regulation', *Progressive Policy Institute*, p. 5.
3 LexisNexis, 'Glossary: Cyberspace definition'. Retrieved from https://www.lexisnexis.co.uk/legal/glossary/cyberspace [accessed 29 November 2023].
4 Article 50 U.S. Code § 1708 (d)(2) - Actions to address economic or industrial espionage in cyberspace.
5 Article 2(3) of the 2018 Law on Cybersecurity.

reality. However, their values inspired the ideal policies and regulatory principles for the future of cyberspace.[6] As cyberspace has no physical border, it raises many questions and debates in international law.

On November 13th 2023, Google filed a case before the United States District Court for the Northern District of California against unknown scammers located in Vietnam and India.[7] These hackers allegedly used false ads on Facebook to download artificial intelligence chatbot Bard. In fact, Bard is a free-access platform of Google without any requirement of download. The scams target small-business owners to steal their control over their business social media accounts by using the malware spread over their devices via the click to linked ads. In this case, Google attempted to block this alleged scheme under the Californian jurisdiction. It is not uncommon in Vietnam that hackers embezzle the business' social network credentials to extort their owners[8] as well as in the US[9] The *Google LLC. v. Does 1-3* case is worth noting because it is unclear how Google can execute the injunction and enforce the US District Court's decision in Vietnam if the US District Court agrees with their requests. Furthermore, it also raises the query concerning Facebook's liability for monetising and suggesting false ads to its users by its algorithms, causing them damages – i.e. Vietnamese business owners and Google who also advertise their products on Facebook.

This case is a concrete example of ransomware of which the victims and unknown hackers are non-State actors located in different countries. It requires the intervention of a legal framework established amongst these countries. For the ransomware amongst the State actors, the following theoretical international law principles may be arguably applied, such as sovereignty, non-intervention, countermeasure, due diligence, international humanitarian law, and human rights. However, those principles appear irrelevant to the ransomware targeting private entities and individuals by non-State hackers, except sovereignty. It is subsequently related to the determination of jurisdiction where the victims can seek prosecution of perpetrators and damage compensation. This paper focuses on the question of the role of international law in protecting the rights of Internet users, especially the applicability of the sovereignty principle to tackle ransomware from varied salient perspectives of several countries and regions. Vietnam

6 Cohn C. (2019), 'Inventing the Future: Barlow and Beyond', *Duke Law & Technology Review*, Vol. 18, p. 77.

7 *Google LLC v. Does 1-3* (2023), U.S. District Court for the Northern District of California, Case No: 5:23-cv-05823.

8 Q. T. (2022), 'Taking over Facebook accounts to extort', *VNExpress*, 25 March 2022.

9 Prado H. D. (2023), 'Taking legal action to protect users of AI and small businesses', *Google blog*. Retrieved from: https://blog.google/outreach-initiatives/public-policy/taking-legal-action-to-protect-users-of-ai-and-small-businesses/ [accessed 29 November 2023]; Alexander J. (2023), 'YouTube sues alleged copyright troll over extortion of multiple YouTubers', *The Verge*. Retrieved from: https://www.theverge.com/2019/8/19/20812144/youtube-copyright-strike-lawsuit-alleged-extortion-minecraft [accessed 29 November 2023].

recently adopted several legal instruments to protect individual fundamental privacy rights and regulate cyberspace. The paper will discuss (i) the theoretical essential principle of international law – sovereignty in cyberspace and questions remaining unanswered about transborder ransomware. Also, it will tackle (ii) the orientation of regulatory measures in the Association of Southeast Asian Nations (ASEAN) region and Vietnam in this matter and analyse Vietnamese legislators' position and its impact.

1. Sovereignty principle in cyberspace

It has been nearly three decades since J.P. Barlow's declaration. It is certain that cyberspace cannot be a free-law zone. However, the absence of a comprehensive set of international laws applicable in cyberspace persists, largely due to significant uncertainties surrounding legal stances and concepts in this domain in many countries.[10] Set apart from the national security problems, the significant challenge of the application of international law principles in the transnational ransomware has been posed and become an interesting subject for the international law experts to investigate. This section will analyse: (i) the fundamental international law principle – sovereignty, which may apply in the case where the ransomware attacks the individuals and private entities across many countries, and (ii) the challenges of regulating the transborder ransomware from legal and practical perspectives, particularly in defining the jurisdiction.

1.1. The applicability of sovereignty principle to ransomware

In 2012, there were several discussions about the application of international law in cyberspace initiated in the US, the United Nations (the UN), and the ASEAN. Accordingly, Prof. Harold H. Koh provided a clear perspective of the US Government on this topic. He affirmed the application of international law principles in cyberspace. Particularly, the sovereignty of other states should be considered. As defined, cyberspace includes not only the Internet, information, cloud storage, etc. but also the network of information technology infrastructure which can be physically located in one nation and cause impacts in other nations. His speech delivered at the US Cyber Command legal conference also predicted the scenario of hacking operations in other States. In addition to sovereignty, enforcement mechanisms also become a difficult query to respond to.[11] The strong gravity of sovereignty was again confirmed by the UN in

10 Cherry L. M., Pascucci P. P. (2023), 'International Law in Cyberspace', in American Bar Association, *An Anthology: 60 Years of Transformation National Security Law*. Retrieved from: https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/ [accessed 29 November 2023]; Homburger, Z. (2019), 'Conceptual Ambiguity of International Norms on State Behaviour in Cyberspace', *EU Cyber Direct – Research In Focus*; Yang M. (2016), 'Legal Ambiguities in Cyberspace', *LawTech.Asia*. Retrieved from: https://lawtech.asia/legal-ambiguities-in-cyberspace/ [accessed 29 November 2023].

11 Koh H. H. (2012), 'International Law in Cyberspace', *Harvard International Law Journal*, Vol. 54, p. 6.

addition to its suggestion of guidelines, and best practices against non-State actors cyberattacks.[12]

Until today, the 22-year-old Budapest Convention retains its influence over the domestic legislation on cybercrime around the world. This Convention inspired legislators of 82% of States in terms of arrangement or partly some relevant notions as their guideline or source.[13] It was adopted on November 23rd, 2001, complemented by its First and Second Additional Protocols adopted on January 28th 2003, and November 17th 2021, setting up a foundation for global cooperation in harmonisation of cybercrime legislation, containing criminal and procedural regulations.[14] Due to the scarcity of relevant authoritative precedents, it is anticipated that there will be efforts to clarify issues of sovereignty and jurisdiction in cyberspace.[15] Despite the endeavour of the Convention's parties, the Convention and its Additional Protocols appear to fail to respond to the main questions of application of international law in cyberspace, i.e. extent, scope and enforcement manner.[16] Particularly, Article 22 of the Convention defining a party's jurisdiction, based on the territorial criterion, was out of date since the arrival of cloud stockage and transborder data flows which allow access to information and devices anywhere without any physical restraints. A grey area of this article may allow the criminal jurisdiction to be extended by the Party's domestic law.[17] However, in cyberspace, the extent of this supplementary provision cannot be determined.[18] It leads to the necessity of discussion about the jurisdiction in ransomware attacks and its connection to the applicability of the sovereignty principle in the next subsection 1.2.

First released in 2013 by Cambridge University Press, the Tallinn Manual encompassed serious cyber activities. Its 2nd version was published in 2017, providing scholarly expertise on the application of international lawin cyberspace. The project of the Tallinn Manual 3.0 has been launched by the North Atlantic Treaty Organization(NATO) Cooperative Cyber Defence Centre of Excellence. The manual's nature is "non-legally binding scholarly work"

12 The U.N. Secretary-General (2013), 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', *U.N. Doc. A/68/98*, 24 June 2013, p. 8, 12.

13 C-PROC (2021), 'The global state of cybercrime legislation 2013 – 2021: A cursory overview', *Europe: Cybercrime Programme Office of the Council of Europe*.

14 Until 2023, Vietnam is not a signatory of the Budapest Convention (ETS No. 185) and its Protocols.

15 Zachar D. (2021), 'Battling Cybercrime Through the New Additional Protocol to the Budapest Convention', *The NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved from: https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/ [accessed 29 November 2023].

16 Cherry L. M., Pascucci P. P., *supra* note 10.

17 Article 22.4 of the Budapest Convention.

18 Rosenberg D. (2022), 'Seizing the means of disruption: international jurisdiction and human rights in the expanding frontier of cyberspace', *International Law and Politics*, Vol. 55, pp. 132-133.

objectively interpreting the application of international law in cyberspace.[19] It remedies the old-fashioned characteristics of the Budapest Convention. While the existing sovereignty definition is restated in the manual, the law experts appealed to the States to clarify their position on sovereignty. The manual used three classic jurisdiction approaches prescriptive, enforcement, adjudicative,[20] to recognise territorial enforcement jurisdiction where the data, cloud server may be accessed or connected, or cyber activities substantially produce impacts. It is arguable to employ the *de minimis* standard to consider the jurisdiction having only a little relation with cyber infrastructure, including data within a State's territory.[21]

Recently, the European Union (EU) is promoting "technological sovereignty' in cybersecurity by proposing co-governed Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres to its Member-States.[22] The EU also looks forward to the partnership with other countries, but there has not been any specific plan outlined at this moment,[23] except for what has been provided by the Budapest Convention (2001) and its Additional Protocols. France acknowledges that the sovereignty principle applies in cyberspace.[24] The nation's sovereignty is exercised over the information systems within French territory.[25] With regard to the need of European cooperation, in 2020, the French Senate proposed to extend the competence of the EU Public Prosecutor's Office over transborder cybercrime in addition to its current responsibility of investigation, prosecution, and judgement against financial interests of the EU.[26] Meanwhile, the United Kingdom (the UK) does not endorse the sovereignty principle which is not considered as a binding rule.[27] It focuses on the non-intervention rule instead in regard to unlawful cyber operations conducted by a State or conducted through non-State actors directed or

19 The NATO Cooperative Cyber Defence Centre of Excellence (2023), 'The Tallinn Manual', *CCDCOE*. Retrieved from https://ccdcoe.org/research/tallinn-manual/ [accessed 6 December 2023].

20 Jensen E. T. (2017), 'The Tallinn Manual 2.0: Highlights and Insights', *Georgetown Journal of International* Law, Vol. 48, pp. 743, 746.

21 Rosenberg D. (2022), *supra* note 16, pp. 137-138.

22 The European Commission (2022), 'Joint Communication to the European Parliament and the Council', *the EU's Cybersecurity Strategy for the Digital Decades*.

23 The European Commission (2022), 'The Cybersecurity Strategy'. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy [accessed 5 December 2023].

24 Cyber Law Toolkit (2019), 'National position of France'. Retrieved from https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#Due_diligence [accessed 30 November 2023].

25 France (2021), 'French position on International Law applied to Operations in Cyberspace', *Paper shared by France with the Open-ended working group established by resolution 75/240*.

26 Sénat (2020), 'Rapport d›information n° 613 (2019-2020)', *Proposition de résolution au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, sur la lutte contre la cybercriminalité : Cybercriminalité : un défi à relever aux niveaux national et européen*, 9 July 2020.

27 Schmitt M. (2021), 'The Sixth United Nations GGE and International Law in Cyberspace', *Just Security*. Retrieved from: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/ [accessed 5 December 2023].

controlled by the State.[28] This leaves another silence on the matters of cyberattacks targeting the non-state actors by non-government-backed cybercriminals.

Like the US and EU, China is one of the leading countries in the information and communication technologies. The country earns between 9.5% - 11.7% market share in the last decade, globally ranked as the third important market.[29] China, as an early proponent, has declared its stance on sovereignty in cyberspace as a principal concept since 2010, advocating for cooperation among nations and endorsing multilateralism in this regard.[30] That explains its orientation to governcyberspace dominated by the sovereignty and the State's control. This proposition is welcomed by the US and EU countries which traditionally pursue the multistakeholder governance.[31] These different approaches have merged into the collaboration between countries to enhance the applicability of the sovereignty principle in cyberspace. In their recent discussion, China brought a thought-provoking perspective on sovereignty, demonstrated by four layered characteristics: *physical, logical, application* and *social* elements. To be more specific, the *physical* one refers to the physical infrastructure facilitating cyberspace. The *logical* element attributes the technical standards, norms for the cyber operation. The *application* relates to the data used for such operation, which could involve the national or social interest. The *social* one indicates the manner that a state governs cyber activities, including the Internet.[32] On the one hand, this perception shows the necessity of the evolution of the sovereignty principle to fit in with the nature of cyberspace, its operation, activities, risks, and impact to society. On the other hand, this notion may be too broad which would very easily create conflict or infringement of the sovereignty of other countries and make the situation more complicated.

28 Braverman S. (2022), 'International Law in Future Frontiers', *Attorney General's Office*. Retrieved from: https://www.gov.uk/government/speeches/international-law-in-future-frontiers [accessed 5 December 2023].

29 Statista Research Department (2023), 'Global ICT market share 2013-2023, by selected country'. Retrieved from: https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/#:~:text=As%20of%202023%2C%20the%20U.S.,share%20of%20over%2011%20percent [accessed 17 December 2023].

30 The Information Office of the State Council of the People's Republic of China (2010), 'The Internet in China', *Information Office of the State Council of the People's Republic of China*. Retrieved from: http://www.china.org.cn/government/whitepaper/node_7093508.htm, pp. 7-8 [accessed 17 December 2023]; Ministry of Foreign Affairs of the People's Republic of China (2021), 'China's Positions on International Rules-making in Cyberspace', 20 October 2021. Retrieved from https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html [accessed 17 December 2023].

31 Gao X. (2022), 'Sovereignty and Cyberspace: China's Ambition to Shape Cyber Norms', *The London School of Economics and Political Science Blogs*. Retrieved from: https://blogs.lse.ac.uk/cff/2022/08/18/sovereignty-and-cyberspace-chinas-ambition-to-shape-cyber-norms/ [accessed 17 December 2023].

32 Kulesza J. (2023), 'Principles of International Law in Cyberspace', *Report on the Third Meeting of the Sino-European Expert Working - Group on the Application of International Law in Cyberspace*, p. 7.

In 1998, in the middle of the dot-com bubble, sovereignty, jurisdiction and cyberspace had been discussed at a very early stage in the context of predictions about the changes in international law made by new technologies, e.g. telecommunication. The discussion favoured contingent sovereignty, suggesting that a State's sovereignty, jurisdiction should be flexibly formed and modified from time to time under its consideration, over conclusory sovereignty as a fixed institution.[33] 25 years later, amid the explosion of artificial intelligence (AI), virtual reality and many advanced information and communication technologies, the agreeable approach of territorial sovereignty remain uncertain. In addition to the recent proposal of Tallinn Manual 3.0, following the manual 2.0, novel approaches to sovereignty and jurisdiction are introduced but common solutions, including determination of their legal nature and application manners, have not been found.[34]

Following regular cyber activities, some proposals were outlined based on the material damages caused by cyberattack (''material damage approach''), potential violation of territorial sovereignty by cyber operation (''intermediate approach''), interference in a State's cyber infrastructure violating its territorial sovereignty by cyber incident (''strict inviolability approach''), and all interruption to the information and communication infrastructure of another State, violating its territorial sovereignty. Amongst these approaches, the author supported the strict inviolability with two-fold requirements. They include a *prima facie* occurrence of sovereignty infringement and its consequence beyond *de minimis* effects.[35] This approach may be rational in the government's position and applicable to the circumstance of the attacks against non-State actors. However, it cannot resolve the case where the private actors use the cloud-based operations or have their cyber infrastructure and data flows through different countries. As a result, other experts came up with a ''norm of de-territorialised data' that eliminates the sovereign government of the numeric data. It is inevitable that this proposition was challenged by the ''norm of sovereign control over data'. It appears contrary to the theory of the ''contingent sovereignty', associated with the ''responsibility to protect' of the State.[36] These suggestions and arguments confirmed the difficulty to find a one-size-fits-all solution to define the sovereignty principle in cyberspace. The absence of a harmonised standard or definition

33 Trachtman J. P. (1998), 'Cyberspace, Sovereignty, Jurisdiction and Modernism', *Indiana Journal of Global Legal Studies*, Vol. 5, No. 2, p. 8.

34 Krasikov D.V, Lipkina, N. N. (2020), 'Sovereignty in Cyberspace: A Scholarly and Practical Discussion', *Advances in Social Science, Education and Humanities Research*, Vol. 498, Proceedings of the XIV European-Asian Law Congress 'The Value of Law'' (EAC-LAW 2020).

35 Chircop L. (2019), 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0', *Melbourne Journal of International Law*, Vol. 14, 2019.

36 Osula A., Rõigas H. (2016), 'International Cyber Norms: Legal, Policy & Industry Perspectives', *NATO Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE), 2016, p. 107-109.

of sovereignty rule, which could suit cyberspace, presents radical challenges to regulate transnational cyberattacks, including ransomware, particularly to define the jurisdiction.

1.2. Jurisdiction: challenge in the regulation of ransomware

The cyberattacks are usually unlimited in terms of border or distance, arduous to ascertain, low-cost and low risk for the hackers. Therefore, the French national cyber security strategy in 2015 focused on the goal of guaranteeing its national sovereignty which was the first of its five goals set.[37] The target to enhance the Member States' and the EU's digital sovereignty was also reflected in the Union's new Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (called as "Directive NIS2').[38] As forecasted by Prof. Harold H. Koh eleven years ago, with the development of cyber activities, especially the numerous and varied cyberattacks, the legal practitioners, judicial, and enforcement agencies are faced with more intricate circumstances.

While sovereignty indicates one State's "complete, exclusive power, authority within the territory", the jurisdiction is connected to the former, "provides the State with the power, authority to define, preserve the duties and rights of people within its territory, enforce the law, and punish violations of laws". Regardless of the interconnectivity between sovereignty and jurisdiction, the jurisdiction is usually defined by domestic law, based on other factual elements (e.g. nationality, residence of offender, victim,...).[39] It is evident that sovereignty has an irrefutable impact on the jurisdiction, especially the jurisdiction to prescribe and enforce. For example, in the context of international contracts regarding cyber activities, the non-State actors may find themselves in a jurisdictional predicament, where their dispute cannot be resolved under one jurisdiction with one applicable law without any prejudice to the rights of other contractual parties. Even though each state wishes to reserve its sovereignty over an uncertain portion of cyberspace, a concept of cyber-jurisdictions has been introduced as a pure international area to cover all disputes over any cyber operation.[40]

37 France Diplomacy (2019), 'France and cyber security'. Retrieved from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/ [accessed 30 November 2023].

38 Yiapanis A., Mazzola A. (2023), 'Opinion of the European Economic and Social Committee on the Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence', *Official Journal of the European Union*, 2023/C 293/04.

39 United Nations Office on Drugs and Crime (2019), 'E4J University Module Series: Cybercrime - Module 7: International Cooperation against Cybercrime'. Retrieved from https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html [accessed 5 December 2023]; Kulesza J., *supra* note 29, p. 8.

40 Adams J., Albakajai M. (2016), 'Cyberspace: A New Threat to the Sovereignty of the State', *Management Studies*, Vol. 4, No. 6, p. 263.

As presented in Part 1.1, Tallinn Manual reused the traditional jurisdiction concepts: (i) "prescriptive jurisdiction' which is "the power to regulate an activity, prescribe certain behaviour", enables the State to legislate for the valid purpose of governing subjects, circumstances; (ii) "enforcement jurisdiction' that a "State's ability to validly enforce its law, through exercise of executive and judicial power", for example the State's authority to arrest, try, convict, gaol its subjects for their violation of its regulations;[41] and, (iii) "adjudicatory jurisdiction', which is a "State's ability to subject persons, things to the process of its courts or administrative tribunals". In general, the "jurisdiction to prescribe" can be claimed on the following grounds: (i) "territoriality", i.e. behaviour is conducted within the territory of the State, or it is outlined to have the consequence within the State's territory; (ii) "nationality", i.e. behaviour is conducted by the State's subjects; (iii) "passive personality", i.e. behaviour's consequence affects the state's subject, its victims; (iv) "protective principle", i.e. behaviour aims to harm the State's interests; and, (v) "universality", i.e. the group of countries consider the behaviour as "universal concern".[42]

In cyberspace, if the sovereignty is de-territorialised, it will raise questions on how to define jurisdiction based on the first principle in the list, territoriality. They lead to a necessary reconsideration of the notion of territorial sovereignty and its current foundational theories in legal systems. Particularly, this territoriality principle is found on the basis that sovereignty can be determined with respect to the extent of a state's jurisdiction. Together with domestic legislation, State sovereignty is governed by the rule encompassing the State's interest outlined jurisdictionally.[43] This standpoint appears to suggest the existence of a "border" in terms of State jurisdiction and sovereignty. In addition, the territoriality principle provides the jurisdiction with a very narrow base. The sole application of one State's jurisdiction to legal relations in cyberspace, for example, based on the location where the consequence following the cyber activity occurs, is inadequate.[44] The multiple jurisdictions or unknown jurisdictions are likely an inevitable result of cyberattacks, occurring and having consequences in many countries. It is extremely difficult to define them and choose the one(s) to apply.

41 Rothwell D. R., Kaye S., Akhtarkhavari A., and Davis R. (2010), 'Jurisdiction', in *International Law: Cases and Materials with Australian Perspectives*, Cambridge University Press, pp. 294–377.

42 American Society of International Law (2014), 'Jurisdictional, Preliminary, and Procedural Concerns', in Diane Marie Amann ed., *Benchbook on International Law* § II.A, American Society of International Law.

43 Gordon S. E. (2001), 'Changing Concepts of Sovereignty and Jurisdiction in the Global Economy: Is there a Territorial Connection?', *Working Paper Series # 1*, p. 4, 28-29.

44 Semenova N. (2021), 'Jurisdiction in Cyberspace'. Retrieved from: http://dx.doi.org/10.2139/ssrn.3912006 [accessed 30 November 2023].

The United Nations' Group of Governmental Experts (GGE) report of 2013 confirmed the relationship between territorial sovereignty and jurisdiction in cyberspace's context: "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of Information and Communication Technology (ICT)-related activities, and to their jurisdiction over ICT infrastructure within their territory".[45] However, it is noteworthy that State sovereignty is distinguishable from the norms, and principles originating in the sovereignty rule itself. In other words, the GGE differentiated the manner of applicability of sovereignty to cyber activities and that of exercising jurisdiction over them.[46] This remarkable standpoint perplexed the relation between sovereignty and jurisdiction. Nevertheless, it may demonstrate the way the jurisdiction should be applied and respect the sovereignty of other States even in the new context having many unknown characteristics like cyberspace.

Going into the details, the great complexity of determining the enforcement, and prescriptive jurisdiction can arise in the case of cyberattacks, especially ransomware targeting the private victims by non-State actors. In common cases where the attackers are possibly traced down within the territory, domestic law may be the legal ground for the victims seeking injunction measures or dispute resolution mechanisms. However, the multiple jurisdictions may place the victims in a predicament. The distinctness between the national regulations can lead to different procedural processes varying from one jurisdiction to another jurisdiction. For example, it is advised for the cyberattack victims in the UK to verify the requirements of other jurisdictions and if the attackers are liable for other sanctions under another jurisdiction.[47] The ramifications of jurisdictions add a major complication to gathering valid electronic evidence due to varied jurisdictions or unknown jurisdictions.[48]

Ransomware designates "a malicious software that, once gaining access and being installed on your device, will encrypt all the data and require a ransom to be paid to return access to the data".[49] Like some other types of cyberattack, the after-effect of ransomware does not come up immediately. In practice, the infiltration by malware into the information systems may take place weeks before the victims' receipt of ransom requests. The payment for data recovery

45 *Supra* note 12.

46 Schmitt M. N., Vihul L. (2017), 'Respect for Sovereignty in Cyberspace', *Texas Law Review,* Vol. 95, No. 3.

47 HM Treasury Office of Financial Sanctions Implementation (2023), 'Ransomware and Sanction – Guidance on Ransomware and Financial Sanctions'. Retrieved from https://assets.publishing.service.gov.uk/media/63e4f0c58fa8f50507f59c16/Ransomware___Sanctions_guidance__Feb_2023_.pdf [accessed 5 December 2023]

48 Kleijssen J., Perri P. (2016), 'Cybercrime, Evidence and Territoriality: Issues and Options', *Netherlands Yearbook of International Law*, Vol. 47, p. 150.

49 The United Nations (2021), 'Ransomware attacks, a growing threat that needs to be countered', *UNODC Regional Office for Southeast Asia and the Pacific.*

or system restoration may be made after a few weeks or up to months. Its consequential damages cannot be precisely measured.[50] It is not certain that any ransom attack amounts to an illegal act. The wrongfulness shall be determined by considering individual circumstances and features of the ransomware, such as its characteristics, extent, results,... Currently, ransomware attacks are majorly managed by the domestic law and most of them are conducted by non-State hackers. Nonetheless, it is still suggested that ransomware should be regulated at the level of international law to protect the interests of both state and non-State actors.[51] While many questions about the application of international law to ransomware operations remain unanswered, Vietnam has made major advances in mitigating, preventing, and stopping cyberattacks, including ransomware.

2. Current cooperative legislative projects and Vietnam's position

In the first six months of 2022, there were 48, 646 cyberattacks in Vietnam.[52] Kaspersky Security Network stated that 41,989,163 cyberattacks were detected and blocked in 2022, decreased by 33,8% in comparison to over 63 million cases in 2021.[53] Although Vietnam is not the country mainly targeted by the ransomware attacks,[54] the country is among the top ten nations which are afflicted the most.[55] Interestingly, in the Global Cybersecurity Index (GCI) of 2020, Vietnam ranked 25th, overall scoring 94.59. In which, its legal and cooperative measures and capacity development are very strong (20/20, 19,26/20).[56] This ranking was much higher than its global rank in 2018 and 2017, which were 50[57] and 100[58] respectively. It is observed that this drastic change was produced because of the introduction of new regulations in 2018. The government sets itself the goal of maintaining the country's GCI ranking amongst top 40 by 2025 and top 30 by 2030 in the respect

50 Cyber Law Toolkit (2023), 'Scenario 14: Ransomware campaign'. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Scenario_14:_Ransomware_campaign#cite_note-7 [accessed 5 December 2023].

51 Akande D., Coco A., Dias T., Hollis D., O'Brien J., and Benthem T. (2021), 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations', *EJIL: Talk!, Just Security and Opinio Juris*, 4 October 2021; *See also:* Lubin A. (2022), 'The Law and Politics of Ransomware', *Vanderbilt Journal of Transnational Law,* Vol. 55, 2021.

52 VnetWork (2023), 'Vietnam's cybersecurity in the first half of 2022', *VnetWork*. Retrieved from: https://www.vnetwork.vn/en-US/news/an-ninh-mang-viet-nam/11 [accessed 30 November 2023].

53 Bao Chinh Phu (2022), 'Cyber Attacks in Vietnam Decrease By Nearly 34% in 2022'. Retrieved from https://en.baochinhphu.vn/cyber-attacks-in-viet-nam-decrease-by-nearly-34-in-2022-11123030910354016-4.htm [accessed 30 November 2023].

54 Flashpoint (2023), 'Flashpoint's Cyber Threat Intelligence Index: Q3 2023 Edition'. Retrieved from https://flashpoint.io/wp-content/uploads/Q3_CTI_Index_2023-final.pdf [accessed 29 November 2023].

55 Griffiths C. (2023), 'The Latest 2023 Ransomware Statistics', *AAG*. Retrieved from: https://aag-it.com/the-latest-ransomware-statistics/ [accessed 29 November 2023].

56 International Telecommunication Union (ITU) (2023), 'Global Cybersecurity Index 2020', Switzerland, 2023.

57 ITU (2018), 'Global Cybersecurity Index 2018'.

58 ITU (2017), 'Global Cybersecurity Index 2017'.

of e-government[59] as a part of organisational and technical measures in the GCI. Vietnam targets that its digital economy will account for 25% of Gross Domestic Product by 2025 and 30% by 2030.[60] The nation also confirms its partnership in regional cybersecurity structure.[61] This section will provide a glance about the country's effort to: (i) enlist regional and international cooperation in respect of the application of international law principle, and (ii) adopt them in its current legal framework of cybersecurity, personal data protection.

2.1. Vietnam's effort in cybersecurity collaboration

As mentioned, the application of international law in cyberspace is not a new discussion topic in the Association of Southeast Asian Nations (ASEAN). There are significant differences between the ASEAN and EU in many aspects of legal culture, legislative structure, and politics which led to many distinct approaches to cybersecurity cooperation. The ASEAN Member States strategically stay at the stage of promoting the need to strengthen cross-sectoral cooperation to ensure the security of ICTs. They outlined a regional action plan on the implementation of the UN Group of Governmental Experts on Advancing responsible State behaviours in cyberspace and the enhanced security measures following the ASEAN Cybersecurity Cooperation Strategy 2021-2025.[62] The strategy focuses on coordination in the region, promotion of international cybersecurity standards, capacity-building measures and establishment of international cooperation.[63] The ASEAN strategy in the application of international law in cyberspace is likely similar to the US,[64] which seemingly maintains its vagueness. The absence of a well-defined notion of sovereignty between the Member States may allow them, including Vietnam, to have the elasticity in their internal and external policy.[65]

In the framework of the ASEAN Ministerial Meeting on Transnational Crime, the Senior Officials Meeting on Transnational Crime Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime

59 Governmental Resolution approval on Project of National Data Center (2023), No. 175/2023/NQ-CP, *Official Gazette*, 1091-1092, 30 October 2023 - Section III.2(e).

60 A. M. (2023), 'Hướng tới mục tiêu kinh tế số chiếm 30% GDP' [trans: 'Aiming for a digital economy to account for 30% of GDP'], *Chinhphu.vn*. Retrived from: https://baochinhphu.vn/huong-toi-muc-tieu-kinh-te-so-chiem-30-gdp-102230914162731311.htm [accessed 29 November 2023].

61 Nguyen V. L. (2020), 'Hợp tác và đấu tranh về an ninh mạng trong quan hệ quốc tế: Cơ hội, thách thức và đề xuất chính sách đối với Việt Nam', *Tạp chí điện tử Cộng sản* [trans: 'Cooperation and Struggle in Cybersecurity in International Relations: Opportunities, Challenges, and Policy Proposals for Vietnam', *Electronic Journal of the Communist Party*]. Retrieved from: https://www.tapchicongsan.org.vn/web/guest/the-gioi-van-de-su-kien/-/2018/816711/hop-tac-va-dau-tranh-ve-an-ninh-mang-trong-quan-he-quoc-te-%C2%A0co-hoi%2C-thach-thuc-va-de-xuat-chinh-sach-doi-voi-viet-nam.aspx [accessed 29 November 2023].

62 ASEAN (2023), 'Chairman's Statement of the 30th ASEAN Regional Forum', 14 July 2023.

63 ASEAN (2021), 'ASEAN Cybersecurity Cooperation Strategy 2021-2025'. Retrieved from https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf [accessed 5 December 2023].

64 Cherry L. M., Pascucci P. P., *supra* note 10.

65 Tan E. E., Ang B. (2022), 'ASEAN Ambiguity on International Law and Norms for Cyberspace', *Baltic Yearbook of International Law Online*, Vol. 20, Issue 1, pp. 134, 147.

encourages the collaboration of Member States with external partners.[66] Particularly, in 2019, the ASEAN and EU together released a statement on cybersecurity operations. They aimed to accelerate the transborder collaboration for tackling crimes and terrorism in cyberspace, encouraging their discussion about the experiences in cyberspace.[67] In 2023, the ASEAN members have enhanced international and regional collaborations with other countries, such as the US, Japan, and China. The 3rd ASEAN-U.S. Cyber Policy Dialogue on February 1st 2023 accelerated their collaboration within the framework of the ASEAN-U.S. Strategic Plan of Action, the ASEAN-U.S. Comprehensive Strategic Partnership, the ASEAN Outlook on the Indo-Pacific, the Master Plan on ASEAN Connectivity 2025.[68] The ASEAN-China Joint Declaration on Cooperation in Support of the ASEAN Comprehensive Recovery Framework of 2021[69] presented the parties' objective to initiate an ASEAN-China Cyber Dialogue and collaboration on technology transfer. Accordingly, it is believed that the China-ASEAN Technology Transfer Centre agreement of 2013 may allow the parties to set up partnerships in cybersecurity.[70] In September 2018, the ASEAN Secretariat, the Government of Thailand, and the Government of Japan formed the ASEAN-Japan Cybersecurity Capacity Building Center to bolster the advancement of ASEAN countries' capacity for cybersecurity. Then, the Japan-ASEAN Technical Cooperation Agreement was signed on May 13th, 2019.[71] Following this agreement, the Japan International Cooperation Agency and the Government of Thailand concluded a Record of Discussions regarding the Project for Enhancing ASEAN-Japan Capacity Building Program for Cybersecurity and Trusted Digital Services.[72]

In addition to the cooperation amongst the ASEAN Member States and its

66 ASEAN, 'Priority Areas of Cooperation'. Retrieved from https://asean.org/our-communities/asean-political-security-community/peaceful-secure-and-stable-region/cyber-security/ [accessed 5 December 2023].

67 EU External Action (2019), 'ASEAN-EU Statement on Cybersecurity Cooperation'. Retrieved from https://www.eeas.europa.eu/node/66196_en [accessed 5 December 2023].

68 Office of the Spokesperson (2023), 'Co-Chairs' Statement on the Fourth ASEAN-U.S. Cyber Policy Dialogue', U.S. Department of State. Retrieved from https://www.state.gov/co-chairs-statement-on-the-fourth-asean-u-s-cyber-policy-dialogue/ [access 5 December 2023].

69 The 24th ASEAN-China Summit on 26 October 2021. Retrieved from https://asean.org/asean-china-joint-statement-on-cooperation-in-support-of-the-asean-comprehensive-recovery-framework/ [accessed 5 December 2023].

70 Ramadhan I. (2023), 'ASEAN-China Cybersecurity Cooperation: Challenges and Opportunities', *Journal of Social and Political Sciences*, Vol. 6, No. 4, p. 7.

71 Ministry of Foreign Affairs of Japan (2019), 'The Signing of the Japan-ASEAN Technical Cooperation Agreement', 13 May 2019. Retrieved from https://www.mofa.go.jp/press/release/press4e_002444.html [accessed 5 December 2023]; See also: 'Agreement on Technical Cooperation between the Association of Southeast Asian Nations and the Government of Japan'. Retrieved from https://asean.org/wp-content/uploads/2012/05/TCA_ASEAN.pdf [accessed 5 December 2023].

72 Japan International Cooperation Agency (2023), 'Signing of Record of Discussions on Technical Cooperation Project with ASEAN Member States: Toward 'a free, fair, and secure cyberspace'' through ASEAN-Japan cooperation', 28 February 2023. Retrieved from https://www.jica.go.jp/Resource/english/news/press/2022/20230228_41.html [accessed 5 December 2023].

partnering countries, Vietnam is active in cooperation with other regions, nations as well as international organisations. Vietnam and the EU released a joint press release, announcing their possible collaboration in the cybersecurity field.[73] Before the joint press release, Vietnam proposed to learn about experiences to secure the information and communication infrastructure, enhance domestic regulations in respect of the nation's sovereignty in cyberspace.[74] Furthermore, Vietnam built up a network of countries and organisations having cyber operations information shared with its agencies.[75] In return, the national agencies may disclose the cybersecurity measures and information in accordance with their bilateral or multilateral agreements.[76]

Following the legislative dissimilarity between the ASEAN and the EU, it is easy to notice that the ASEAN does not establish a regional institute as an independent authority governing the cybersecurity cooperation (e.g. technical control, norms, standards establishment) of its Member States due to its political nature.[77] Southeast Asia, including the Vietnam market is well-known as one of the global tech hubs, notably for technology start-ups.[78] These factors require Vietnam to establish more technical support channels and seek for more collaborative resources. Following the formalisation of regional cooperation of Computer Emergency Response Teams (CERTs) in the early 2000s, Vietnam Computer Emergency Team (VNCERT) was established in 2005, and its operation is governed by the Ministry of Information and Communications (MIC). It manages the coordination of cyber incidents, formation of technical standards, conformity, development of Computer emergency response team (CERT), Computer security incident response team (CSIRT) and cooperation with international CERTs.[79] VNCERT also collaborates with other non-State actors in order to improve its coordination and training program.[80] For example, it participates in the "Information Sharing Working Group' of the "\Asia Pacific

73 European Union External Action (2023), 'EU-Vietnam: joint press release for the 4th EU-Vietnam Joint Committee', EEAS, 27 October 2023. Retrieved from https://www.eeas.europa.eu/eeas/eu-vietnam-joint-press-release-4th-eu-vietnam-joint-committee_en [accessed 5 December 2023]

74 Vietnamplus (2022), 'Vietnam asks for EU's stronger support in cyber security protection', 28 April 2022. Retrieved from https://en.vietnamplus.vn/vietnam-asks-for-eus-stronger-support-in-cyber-security-protection/227696.vnp [accessed 5 December 2023].

75 Information Security Department, 'Some countries and organizations have cybersecurity information sharing to Viet Nam'. Retrieved from https://ais.gov.vn/CERT-global-and-VNCERT_pdf.pdf [accessed 5 December 2023].

76 Information Security Department, 'Gci Cybersecurity Cooperation'. Retrieved from https://ais.gov.vn/gci-cybersecurity-cooperation.html [accessed 5 December 2023].

77 Tay K. L. (2023), 'ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework', *The International Institute for Strategic Studies*, p. 13.

78 Vyas R. K. (2022), '3 Reasons Southeast Asia Is A Hot Market For Tech Startups', *Forbes*, 17 May 2022.

79 Retrieved from: https://www.first.org/members/teams/vncert, https://vncert.vn [accessed 30 November 2023].

80 Nguyen H. (2018), 'PwC Vietnam and VNCERT form strategic partnership for cyber security incident response', *Vietnam Investment Review*, 2018.

Computer Emergency Response Team (APCERT),[81] Information Sharing Working Group' within the ASEAN Emergency Response and Assessment Team (ASEAN-ERAT).[82]

In the case of transnational cyberattacks, including ransomware, the hackers may be based in a country other than Vietnam. In 2017, Vietnam was among 20 countries affected by the infamous WannaCry ransomware, which was associated with the Lazarus Group, known to have connections with the North Korean government.[83] These schemes enable the information to erratically cross the borders of many jurisdictions. As a result, it could be a tough challenge for the non-State victims to determine an appropriate jurisdiction[84] and then seek an injunction and damage compensation. It also creates difficulties for Vietnamese authorities to detect the hackers, to trace the information and evidence because of differences in regulations, language barriers, and confidential obligations of the service providers toward their clients.[85] There is a limit on the number of countries, having mutual legal assistance conventions and agreements on extradition with Vietnam. Until 2021, Vietnam signed 12 conventions on general mutual legal assistance, 01 convention on general mutual legal assistance in civil matters, 14 conventions on mutual legal assistance in criminal matters, 14 agreements on extradition, and 15 agreements on the transfer of people serving imprisonment sentences.[86] Through many years, Vietnam authorities used several agreements to gather information about cybercrime.[87] It is witnessed that Vietnam's government makes constant efforts to enhance collaboration with various actors to protect the security of

81 Asia Pacific Computer Emergency Response Team (APCERT) (2019), 'APCERT Annual Report 2019', 2019.

82 ASEAN (2020), 'Chairman's Statement of the 36th ASEAN Summit 26 June 2020 Cohesive and Responsive ASEAN', 26 June 2020. Retrieved from: https://asean.org/wp-content/uploads/2020/06/Chairman-Statement-of-the-36th-ASEAN-Summit-FINAL.pdf [accessed 5 December 2023]

83 Reuters (2017), 'In Vietnam and across Asia, hard lessons for ransomware victims', *Vnexpress*. Retrieved from: https://e.vnexpress.net/news/news/in-vietnam-and-across-asia-hard-lessons-for-ransomware-victims-3585383.html [accessed 30 November 2023].

84 Perloff-Giles A. (2018), 'Transnational Cyber Offenses: Overcoming Jurisdictional Challenges', *The Yale Journal of International Law,* Vol. 43, p. 196.

85 Cao A. D., Ngo T. B. T. (2021), 'Biện pháp thu thập, chuyển hóa, sử dụng chứng cứ điện tử trong vụ án sử dụng công nghệ cao' [trans: 'Measures for Collecting, Transforming, and Using Electronic Evidence in High-Tech Criminal Cases'], *Supreme People's Procuracy of Vietnam*, Retrieved from: https://tapchitoaan.vn/bien-phap-thu-thap-chuyen-hoa-su-dung-chung-cu-dien-tu-trong-vu-an-su-dung-cong-nghe-cao5605.html [accessed 30 November 2023].

86 Official Dispatch on mutual legal assistance, service abroad of judicial documents of the Supreme People's Court No. 33/TANDTC-HTQT, 17 March 2021.

87 Cao A. D., Ngo T. B. T., *supra* note 85. Case 'Pham Ngoc Van, Fraudulent appropriation of property through an online commodity trading platform', Ho Chi Minh, 2011. In the investigation into Tran Bac Ha's fraudulent appropriation of property of Tien Phong commercial bank, 2019, the authorities applied the mutual legal assistance agreement with Slovenia to collect the information of cybercrime – Vietnam's Government, 'Report on the activities of mutual legal assistance in 2019', No. 479/BC-CP, 12 October 2019. Retrieved from https://congan.com.vn/tin-chinh/thu-thap-chung-cu-ve-hanh-vi-gui-tien-qua-lao-va-campuchia-cua-tran-bac-ha_81536.html [accessed 30 November 2023].

cyberspace. As a central principle, any collaboration must respect sovereignty.[88] It appears that Vietnam reciprocally applies this rule in collaborations with other countries. Additionally, the establishment of inclusive legislation on cyberspace and encouragement of compliance with international law is considered the nation's accomplishment in recognising the sovereignty principle.[89]

2.2. Vietnam's position on the protection of cybersecurity against ransomware

To reinforce national cybersecurity, Vietnam has recently introduced significant laws and regulations. The adoption of Law No. 24/2018/QH14 on Cybersecurity (the 2018 Cybersecurity Law) was considered a public statement of the nation's sovereignty protection.[90] From the external viewpoint, this law encompasses data localisation and online content governance.[91] Prior to this 2018 Cybersecurity Law, Law No. 86/2015/QH13 on Cyberinformation Security (the 2015 Cyberinformation Security Law) was released in 2015 to protect online information, the information systems from unlawful access, use, disclosure, interruption, modification or destruction of information and ensure the entirety, confidentiality and feasibility of such information.[92] In addition to the protection of the entirety, confidentiality, and feasibility of the cyber data, the former in 2015 aimed to ensure national security and public order, which are the main differences between the two bills. Meanwhile, the latter in 2018 targets more individual Internet users.[93] Last year, a new Decree No. 53/2022/ND-CP detailing the 2018 Cybersecurity Law provided the measures and procedures protecting national cybersecurity.

Following the 2015 Cyberinformation Security Law, the Decree on Penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions No. 15/2020/ND-CP and Decree No. 14/2022/ND-CP amending Decree 15/2020/ND-CP were established to specify the administrative contraventions of 2015 Cyberinformation Security Law and others and the corresponding sanctions and remedy measures. Currently, the third draft of the

88 Law on Cybersecurity (2018), No. 24/2018/QH14, *Official Gazette,* 775-776, 12 June 2018, pp. 42-73 - Article 7.1. *Law on Cyberinformation Security* (2015), No. 86/2015/QH13, *Official Gazette*, 1239-1240, 19 November 2015, pp. 3-30 - Article 6.1(a).

89 Security Council (2021), 'Explosive' Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats', SC/14563, 29 June 2021.

90 Vu T. T. Anh (2023), 'Protecting Vietnam's Sovereignty in Cyberspace: Insights from Human Right Laws', *The Age of Human Rights Journal*, Vol. 21, p. 15.

91 Wen R. (2019), 'Vietnam's New Cybersecurity Law: A Headache for US Service Providers?', *Georgetown Law Technology Review*. Retrieved from: https://georgetownlawtechreview.org/vietnams-new-cybersecurity-law-a-headache-for-us-service-providers/GLTR-02-2019/ [accessed 5 December 2023].

92 Article 3.1 of the 2015 Law on Cyberinformation Security.

93 Van Ly (2018), 'Quốc hội: Hợp nhất luật an ninh mạng và an toàn thông tin là không khả thi' [trans: Congress: Consolidating cybersecurity and information security laws is not feasible], *The Saigon Times*. Retrieved from: https://thesaigontimes.vn/quoc-hoi-hop-nhat-luat-an-ninh-mang-va-an-toan-thong-tin-la-khong-kha-thi/ [accessed 5 December 2023].

decree stipulating the administrative contraventions of the 2018 Cybersecurity Law, sanctions and remedy measures was published for public consultations. This proposed decree will modify Decree No. 15/2020 ND-CP and cover the administrative contravention of personal data regulations. Currently, Decree No. 15/2020 governs the ransomware attack with the ransom lower than 2 million Vietnam dong or without ransom demand.[94] On the one hand, these regulations on administration contravention of cyberattacks can be applied not only to Vietnamese individuals and entities but also to foreign ones.[95] On the other hand, the foreign organisations and individuals would refer to the expats and international entities residing, and operating within Vietnam's territory under the older Decree No. 25/2014/ND-CP.[96] The later approach could reach the greatest extent of jurisdiction over the administrative violation of cyber operations.

Like many countries (e.g. Australia, France),[97] Vietnam also criminalises ransomware in domestic legal systems even if the country is not a member of the Budapest Convention.[98] It is observed in practice that ransomware is usually detected and investigated by the police. Vietnam's 2015 Penal Code (2015 Penal Code) dedicates a whole section regulating "the offences against regulation on information technology and telecommunications network". Ransomware, including ransom payment, is classed as a wrongful act of establishing or

94 Articles 80.2, 81.2 of the Decree on Penalties for Administrative Violations against Regulations on Postal Services, Telecommunications, Radio Frequencies, Information Technology and Electronic Transactions, No 15/2020/ND-CP, Official Gazette, 217-218, 16 February 2020; Decree amending Decree 15/2020/ND-CP regulating penalties for administrative violations in the fields of postal, telecommunications, radio frequency, information technology and transactions electronics and Decree 119/2020/ND-CP regulating penalties for administrative violations in journalism and publishing activities, No. 14/2022/ND-CP, Official Gazette, pp. 223-224, 9 February 2022.

95 Article 2 of the Decree on Penalties for Administrative Violations against Regulations on Postal Services, Telecommunications, Radio Frequencies, Information Technology and Electronic Transactions, No 15/2020/ND-CP, Official Gazette, 217-218, 16 February 2020; Article 2 of the Draft decree ver. 3.0 on Regulations on Penalties for Administrative Violations in the Field of Cyber Security (2023).

96 Article 2 of the Decree on prescribing the prevention and combat against crimes and violation of other law regarding information technology (2014), No. 25/2014/ND-CP, *Official Gazette*, 449-450, 17 April 2014.

97 Lai B. (2022), 'The threat of ransomware', Parliament of Australian. Retrieved from: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook47p/ThreatRansomware [accessed 5 December 2023]; Piper A. (2022), 'The rights and wrongs of ransomware', *International Bar Association*. Retrieved from: https://www.ibanet.org/The-rights-and-wrongs-of-ransomware [accessed 5 December 2023]; Articles 313-1 to 313-3, 323-2 of French Penal Code (1992), No. 92-685, *Official Gazette*, 169, 23 July 1992, modified in 2000, 2013, 2015 respectively; Australia's Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022 (the Bill) amending the Criminal Code Act 1995 (Criminal Code), Crimes Act 1914 and Proceeds of Crime Act 2002 (POCA).

98 Council of Europe Portal (2022), 'Ransomware: New Guidance Note by the T-CY'. Retrieved from: https://www.coe.int/en/web/cybercrime/-/ransomware-new-guidance-note-by-the-t-cy [accessed 5 December 2023].

providing telecommunications or Internet services for property appropriation.[99] Both Cybersecurity Law and Cyberinformation Security Law distinguish amongst disciplinary measures, administrative sanctions and prosecution based on the nature and level of violation.[100] The enforcement jurisdiction shall be determined by the seriousness and consequence of ransomware acts which are sorted out by the decrees on penalties imposed for administrative violations in information technology, particularly cybersecurity, and then for cybercrime. Adopting a similar approach to the decrees on administrative contraventions of cyberattacks, the 2015 Penal Code maximises its extent of jurisdiction to protect the interest of Vietnamese individuals, and organisations within its territory.[101] For the civil matters of the attack, the 2015 Civil Code may intervene; however, it seems not likely to separate the ransomware into civil and penal cases.

It is observed that the European countries place responsibility on the data controller(s) and processor(s) for informing the authorities and victims of the cyberattacks about personal data breaches.[102] Learning from this legislative experience, Vietnam's adoption of Decree No. 13 on Personal Data Protection, on April 17th, 2023 (Decree No. 13/2023) also represents a significant leap in privacy protection. This decree compels data controllers and processors to report data breaches to law enforcement agencies, specifically the Department of Cybersecurity and Hi-tech Crime Prevention under the Ministry of Public Security.[103] The direct involvement of law enforcement can streamline processes and reduce the time taken to address and resolve data breaches, which is

99 Penal Code (2015), No. 100/2015/QH13, *Official Gazette, 1263-1264, 1265-1266, 1267-1268, 1269-1270*, 27 November 2015 - Article 290.1(dd); Quang Binh Province First Instance Court (2021), *Illegally establishing or providing telecommunications or Internet services for the purpose of property appropriation*, No. 26/2021/HS-ST; See also Nguyen M. V., Le T. H. (2023), 'Tội phạm sử dụng công nghệ cao; những khó khăn, vướng mắc trong phòng, chống và xử lý' [trans: 'Crime uses high technology; difficulties and problems in prevention, control and handling'], *Room 2 – People's Procuracy of Hai Duong province*, 13 October 2023.

100 Article 9 of the 2018 Law on Cybersecurity; Article 8 of the 2015 Law on Cyberinformation Security.

101 Chapter II of the 2015 Penal Code.

102 Articles 4.12, 32, 33, 55 of the Regulation (EU) (2016) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*General Data Protection Regulation*, GDPR), No. 2016/679, *Official Journal of the European Union*, L 119/1, 4 May 2016; Article 16.3 of the Directive (EU) (2016) of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, No. 2016/1148, *Official Journal of the European Union*, L 194/1, 19 July 2016; *See also*: European Data Protection Board (EDPB) (2023), 'Guidelines 9/2022 on personal data breach notification under GDPR', ver. 2.0, 28 March 2023, pp. 31; CNIL (2021), 'Multiplication des attaques par rançongiciel: comment limiter les risques?' [Ransomware attacks on the increase: how can you limit the risks?], 23 April 2021. Retrieved from: https://www.cnil.fr/fr/multiplication-des-attaques-par-rancongiciel-comment-limiter-les-risques [accessed 18 December 2023]; Agencia español protección datos (AEPD) (2020), 'Personal data breaches: Ransomware and risk management'. Retrieved from: https://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/4/crossheading/obligations-relating-to-personal-data-breaches/enacted [accessed 5 December 2023]; UK's Data Protection Act of 2018 – Part 3 (Law Enforcement Processing) Chapter 4 (Controller and Processor) Obligations relating to personal data breaches.

103 Article 23 of the Decree No. 13/2023 on Personal Data Protection.

essential in the fast-paced digital world. A key difference between the European and Vietnamese approaches lies in the role of the Data Protection Authority (DPA). For instance, in the UK, the Information Commissioner's Office is "an independent body upholding information rights";[104] and in France, the Data Protection Authority (CNIL) is "an independent administrative authority found under the Data Protection Act of 1978".[105] According to the European Commission, the "DPAs are independent public authorities that supervise, through investigate and corrective powers, the application of the data protection law".[106] The independent nature of these authorities, which is dissimilar to administration, allows them to provide opinions, suggestions, some legislative measures, make their own decisions, or impose penalties.[107] Contrastingly, in Vietnam, the approach to data breaches is viewed predominantly through the lens of potential cybercrime. This perspective has shaped the legal framework, empowering the police to handle issues of national sovereignty, including cyberspace and information rights, more effectively and efficiently than an independent authority. Consequently, the police in Vietnam have a more exclusive role, extending beyond cyberspace to encompass broader aspects of information rights. The police's involvement emphasizes the importance of protecting not only individual data rights but also the integrity of national digital assets. However, the police's exclusive role in handling all aspects of data breaches and cybercrime might lead to an overreach of administrative authority.

Conclusion

Today, the whole world must deal with cyberattacks, including ransomware. The targets are frequently the most vulnerable but also the most significant actors in society, including both state and non-State actors. In cyberspace, it seems likely not to have any border which could refrain the hackers and powerful organisations, bodies behind them. The traditional international law principles play an important role in governing the virtual world. However, its application is much more troublesome in complex incidents, especially those of non-state actors. In such cases, sovereignty allows the governments to regulate ransomware and cyberattacks in general, and provide the bodies in charge with the measures to detect, investigate and sanction the cybercriminals. Moreover,

104 ICO, 'Who we are'. Retrieved from: https://ico.org.uk/about-the-ico/who-we-are/ [accessed 5 December 2023].

105 CNIL (2023), 'Status & Composition'. Retrieved from: https://www.cnil.fr/en/cnil/status-composition [accessed 5 December 2023].

106 European Commission (EC), 'What are Data Protection Authorities (DPAs)?'. Retrieved from: https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en [accessed 18 December 2023].

107 Contis N., Doguet C. (2020), 'Members of independent administrative authorities can be recused under principle of impartiality', *Lexology*. Retrieved from: https://www.lexology.com/commentary/litigation/france/kalliop/members-of-independent-administrative-authorities-can-be-recused-under-principle-of-impartiality [accessed 18 December 2023].

sovereignty is associated with the jurisdiction under which the non-State actors can report, seek for an injunction, and claim damages. On one hand, some States propose modernised notions and the extent of sovereignty principle which are adapted to the nature of cyberspace. On the other hand, well-calculated silence on the application of this principle let some other states retain the litheness in diplomatic policy.

Vietnam has become an attractive destination for tech start-ups. Its young industry of information and communication technology has suffered from cyberattacks, particularly ransomware. Its government has made a great effort to work with other countries, regional and international organisations to engage in fierce combat against cybercrime. The international law principles, notably the sovereignty, underly these partnerships. In addition, Vietnam's recent regulations on cybersecurity intently protect its inexperienced but very promising ICT business. Cyberspace has its own perplexing and unexplained characteristics. Like other nations, Vietnam's governmental bodies need to deepen their knowledge and acquire more technical skills to prevent, investigate and fight the complex transnational ransomware and other cyberattacks. Furthermore, non-State actors may require a mechanism from the government that provides security norms and technical support. This guidance would help them exercise their rights and ensure an advanced legal framework is in place to protect their intellectual properties and their consumers' rights, particularly concerning personal information. ●

References

**** Case law***

[1] *Google LLC v. Does 1-3* (2023), U.S. District Court for the Northern District of California, Case No: 5:23-cv-05823

[2] Quang Binh Province First Instance Court (2021), *Illegally establishing or providing telecommunications or Internet services for the purpose of property appropriation*, No. 26/2021/HS-ST

****Books and articles***

[3] A. M. (2023), 'Hướng tới mục tiêu kinh tế số chiếm 30% GDP' [trans: 'Aiming for a digital economy to account for 30% of GDP'], *Chinhphu.vn*. Retrieved from: https://baochinhphu.vn/huong-toi-muc-tieu-kinh-te-so-chiem-30-gdp-102230914162731311.htm [accessed 29 November 2023]

[4] Adams J., Albakajai M. (2016), 'Cyberspace: A New Threat to the Sovereignty of the State', *Management Studies*, Vol. 4, No. 6

[5] Agencia español protección datos (AEPD) (2020), 'Personal data breaches: Ransomware and risk management'. Retrieved from: https://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/4/crossheading/obligations-relating-to-personal-data-breaches/enacted [accessed 5 December 2023]

[6] Akande D., Coco A., Dias T., Hollis D., O'Brien J., and Benthem T. (2021), 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of

Ransomware Operations', *EJIL: Talk!, Just Security and Opinio Juris*, 4 October 2021
[7] Alexander J. (2023), 'YouTube sues alleged copyright troll over extortion of multiple YouTubers', *The Verge*. Retrieved from: https://www.theverge.com/2019/8/19/20812144/youtube-copyright-strike-lawsuit-alleged-extortion-minecraft [accessed 29 November 2023]
[8] American Society of International Law (2014), 'Jurisdictional, Preliminary, and Procedural Concerns', in Diane Marie Amann ed., *Benchbook on International Law* § II.A, American Society of International Law
[9] ASEAN, 'Priority Areas of Cooperation'. Retrieved from https://asean.org/our-communities/asean-political-security-community/peaceful-secure-and-stable-region/cyber-security/ [accessed 5 December 2023]
[10] ASEAN (2021), 'ASEAN Cybersecurity Cooperation Strategy 2021-2025'. Retrieved from https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf [accessed 5 December 2023]
[11] ASEAN (2020), 'Chairman's Statement of the 36th ASEAN Summit 26 June 2020 Cohesive and Responsive ASEAN', 26 June 2020. Retrieved from: https://asean.org/wp-content/uploads/2020/06/Chairman-Statement-of-the-36th-ASEAN-Summit-FINAL.pdf [accessed 5 December 2023]
[12] ASEAN (2023), 'Chairman's Statement of the 30th ASEAN Regional Forum', 14 July 2023
[13] Asia Pacific Computer Emergency Response Team (APCERT) (2019), 'APCERT Annual Report 2019', 2019
[14] Barlow J. P. (1996), 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/cyberspace-independence [accessed 29 November 2023]
[15] Bao Chinh Phu (2022), 'Cyber Attacks in Vietnam Decrease By Nearly 34% in 2022'. Retrieved from https://en.baochinhphu.vn/cyber-attacks-in-viet-nam-decrease-by-nearly-34-in-2022-11123030910354016-4.htm [accessed 30 November 2023]
[16] Braverman S. (2022), 'International Law in Future Frontiers', *Attorney General's Office*. Retrieved from: https://www.gov.uk/government/speeches/international-law-in-future-frontiers [accessed 5 December 2023]
[17] C-PROC (2021), 'The global state of cybercrime legislation 2013 – 2021: A cursory overview', *Europe: Cybercrime Programme Office of the Council of Europe*
[18] Cao A. D., Ngo T. B. T. (2021), 'Biện pháp thu thập, chuyển hóa, sử dụng chứng cứ điện tử trong vụ án sử dụng công nghệ cao' [trans: 'Measures for Collecting, Transforming, and Using Electronic Evidence in High-Tech Criminal Cases'], *Supreme People's Procuracy of Vietnam*, Retrieved from: https://tapchitoaan.vn/bien-phap-thu-thap-chuyen-hoa-su-dung-chung-cu-dien-tu-trong-vu-an-su-dung-cong-nghe-cao5605.html [accessed 30 November 2023].
[19] Cherry L. M., Pascucci P. P. (2023), 'International Law in Cyberspace', in American Bar Association, *An Anthology: 60 Years of Transformation National Security Law*. Retrieved from: https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/ [accessed 29 November 2023]
[20] Chircop L. (2019), 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0', *Melbourne Journal of International Law*, Vol. 14, 2019
[21] CNIL (2021), 'Multiplication des attaques par rançongiciel : comment limiter les

risques?' [Ransomware attacks on the increase: how can you limit the risks?], 23 April 2021. Retrieved from: https://www.cnil.fr/fr/multiplication-des-attaques-par-rancongiciel-comment-limiter-les-risques [accessed 18 December 2023]

[22] CNIL (2023), 'Status & Composition'. Retrieved from: https://www.cnil.fr/en/cnil/status-composition [accessed 5 December 2023]

[23] Cohn C. (2019), 'Inventing the Future: Barlow and Beyond', *Duke Law & Technology Review*, Vol. 18

[24] Contis N., Doguet C. (2020), 'Members of independent administrative authorities can be recused under principle of impartiality', *Lexology*. Retrieved from: https://www.lexology.com/commentary/litigation/france/kalliop/members-of-independent-administrative-authorities-can-be-recused-under-principle-of-impartiality [accessed 18 December 2023].

[25] Council of Europe Portal (2022), 'Ransomware: New Guidance Note by the T-CY'. Retrieved from: https://www.coe.int/en/web/cybercrime/-/ransomware-new-guidance-note-by-the-t-cy [accessed 5 December 2023]

[26] Cyber Law Toolkit (2019), 'National position of France'. Retrieved from https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#Due_diligence [accessed 30 November 2023]

[27] Cyber Law Toolkit (2023), 'Scenario 14: Ransomware campaign'. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Scenario_14:_Ransomware_campaign#cite_note-7 [accessed 5 December 2023]

[28] Ehrlich E. (2014), 'A Brief history of Internet regulation', *Progressive Policy Institute*

[29] European Commission (EC), 'What are Data Protection Authorities (DPAs)?'. Retrieved from: https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en [accessed 18 December 2023]

[30] European Data Protection Board (EDPB) (2023), 'Guidelines 9/2022 on personal data breach notification under GDPR', ver. 2.0, 28 March 2023

[31] EU External Action (2019), 'ASEAN-EU Statement on Cybersecurity Cooperation'. Retrieved from https://www.eeas.europa.eu/node/66196_en [accessed 5 December 2023]

[32] European Union External Action (2023), 'EU-Vietnam: joint press release for the 4th EU-Vietnam Joint Committee', EEAS, 27 October 2023. Retrieved from https://www.eeas.europa.eu/eeas/eu-vietnam-joint-press-release-4th-eu-vietnam-joint-committee_en [accessed 5 December 2023]

[33] Flashpoint (2023), 'Flashpoint's Cyber Threat Intelligence Index: Q3 2023 Edition'. Retrieved from https://flashpoint.io/wp-content/uploads/Q3_CTI_Index_2023-final.pdf [accessed 29 November 2023]

[34] France Diplomacy (2019), 'France and cyber security'. Retrieved from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/ [accessed 30 November 2023]

[35] France (2021), 'French position on International Law applied to Operations in Cyberspace', *Paper shared by France with the Open-ended working group established by resolution 75/240*.

[36] Gao X. (2022), 'Sovereignty and Cyberspace: China's Ambition to Shape Cyber Norms', *The London School of Economics and Political Science Blogs*. Retrieved from: https://blogs.lse.ac.uk/cff/2022/08/18/sovereignty-and-cyberspace-chinas-ambition-to-shape-cyber-norms/ [accessed 17 December 2023]

[37] Gordon S. E. (2001), 'Changing Concepts of Sovereignty and Jurisdiction in the Global Economy: Is there a Territorial Connection?', *Working Paper Series # 1*
[38] Governmental Resolution approval on Project of National Data Center (2023), No. 175/2023/NQ-CP, *Official Gazette*, 1091-1092, 30 October 2023 - Section III.2(e)
[39] Griffiths C. (2023), 'The Latest 2023 Ransomware Statistics', *AAG*. Retrieved from: https://aag-it.com/the-latest-ransomware-statistics/ [accessed 29 November 2023]
[40] HM Treasury Office of Financial Sanctions Implementation (2023), 'Ransomware and Sanction – Guidance on Ransomware and Financial Sanctions'. Retrieved from https://assets.publishing.service.gov.uk/media/63e4f0c58fa8f50507f59c16/Ransomware___Sanctions_guidance__Feb_2023_.pdf [accessed 5 December 2023]
[41] Homburger, Z. (2019), 'Conceptual Ambiguity of International Norms on State Behaviour in Cyberspace', *EU Cyber Direct – Research In Focus*
[42] ICO, 'Who we are'. Retrieved from: https://ico.org.uk/about-the-ico/who-we-are/ [accessed 5 December 2023]
[43] Information Security Department, 'Gci Cybersecurity Cooperation'. Retrieved from https://ais.gov.vn/gci-cybersecurity-cooperation.html [accessed 5 December 2023]
[44] Information Security Department, 'Some countries and organizations have cybersecurity information sharing to Viet Nam'. Retrieved from https://ais.gov.vn/CERT-global-and-VNCERT_pdf.pdf [accessed 5 December 2023]
[45] International Telecommunication Union (ITU) (2023), 'Global Cybersecurity Index 2020', Switzerland, 2023
[46] ITU (2018), 'Global Cybersecurity Index 2017'
[47] ITU (2018), 'Global Cybersecurity Index 2018'.
[48] Japan International Cooperation Agency (2023), 'Signing of Record of Discussions on Technical Cooperation Project with ASEAN Member States: Toward 'a free, fair, and secure cyberspace" through ASEAN-Japan cooperation', 28 February 2023. Retrieved from https://www.jica.go.jp/Resource/english/news/press/2022/20230228_41.html [accessed 5 December 2023]
[49] Jensen E. T. (2017), 'The Tallinn Manual 2.0: Highlights and Insights', *Georgetown Journal of International* Law, Vol. 48
[50] Kleijssen J., Perri P. (2016), 'Cybercrime, Evidence and Territoriality: Issues and Options', *Netherlands Yearbook of International Law*, Vol. 47
[51] Koh H. H. (2012), 'International Law in Cyberspace', *Harvard International Law Journal*, Vol. 54
[52] Krasikov D.V, Lipkina, N. N. (2020), 'Sovereignty in Cyberspace: A Scholarly and Practical Discussion', *Advances in Social Science, Education and Humanities Research*, Vol. 498, Proceedings of the XIV European-Asian Law Congress 'The Value of Law" (EAC-LAW 2020)
[53] Kulesza J. (2023), 'Principles of International Law in Cyberspace', *Report on the Third Meeting of the Sino-European Expert Working - Group on the Application of International Law in Cyberspace*
[54] Lai B. (2022), 'The threat of ransomware', Parliament of Australian. Retrieved from: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook47p/ThreatRansomware [accessed 5 December 2023]
[55] LexisNexis, 'Glossary: Cyberspace definition'. Retrieved from https://www.lexisnexis.co.uk/legal/glossary/cyberspace [accessed 29 November 2023]

[56] Lubin A. (2022), 'The Law and Politics of Ransomware', *Vanderbilt Journal of Transnational Law,* Vol. 55, 2021

[57] Ministry of Foreign Affairs of Japan (2019), 'The Signing of the Japan-ASEAN Technical Cooperation Agreement', 13 May 2019. Retrieved from https://www.mofa.go.jp/press/release/press4e_002444.html [accessed 5 December 2023]

[58] Nguyen H. (2018), 'PwC Vietnam and VNCERT form strategic partnership for cyber security incident response', *Vietnam Investment Review*, 2018

[59] Nguyen M. V., Le T. H. (2023), 'Tội phạm sử dụng công nghệ cao; những khó khăn, vướng mắc trong phòng, chống và xử lý' [trans: 'Crime uses high technology; difficulties and problems in prevention, control and handling'], *Room 2 – People's Procuracy of Hai Duong province*, 13 October 2023

[60] Nguyen V. L. (2020), 'Hợp tác và đấu tranh về an ninh mạng trong quan hệ quốc tế: Cơ hội, thách thức và đề xuất chính sách đối với Việt Nam', *Tạp chí điện tử Cộng sản* [trans: 'Cooperation and Struggle in Cybersecurity in International Relations: Opportunities, Challenges, and Policy Proposals for Vietnam', *Electronic Journal of the Communist Party*]. Retrieved from: https://www.tapchicongsan.org.vn/web/guest/the-gioi-van-de-su-kien/-/2018/816711/hop-tac-va-dau-tranh-ve-an-ninh-mang-trong-quan-he-quoc-te-%C2%A0co-hoi%2C-thach-thuc-va-de-xuat-chinh-sach-doi-voi-viet-nam.aspx [accessed 29 November 2023]

[61] Office of the Spokesperson (2023), 'Co-Chairs' Statement on the Fourth ASEAN-U.S. Cyber Policy Dialogue', U.S. Department of State. Retrieved from https://www.state.gov/co-chairs-statement-on-the-fourth-asean-u-s-cyber-policy-dialogue/ [access 5 December 2023]

[62] Osula A., Rõigas H. (2016), 'International Cyber Norms: Legal, Policy & Industry Perspectives', *NATO Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE), 2016

[63] Perloff-Giles A. (2018), 'Transnational Cyber Offenses: Overcoming Jurisdictional Challenges', *The Yale Journal of International Law,* Vol. 43

[64] Piper A. (2022), 'The rights and wrongs of ransomware', *International Bar Association*. Retrieved from: https://www.ibanet.org/The-rights-and-wrongs-of-ransomware [accessed 5 December 2023]

[65] Prado H. D. (2023), 'Taking legal action to protect users of AI and small businesses', *Google blog*. Retrieved from: https://blog.google/outreach-initiatives/public-policy/taking-legal-action-to-protect-users-of-ai-and-small-businesses/ [accessed 29 November 2023]

[66] Q. T. (2022), 'Taking over Facebook accounts to extort', *VNExpress*, 25 March 2022

[67] Ramadhan I. (2023), 'ASEAN-China Cybersecurity Cooperation: Challenges and Opportunities', *Journal of Social and Political Sciences*, Vol. 6, No. 4

[68] Reuters (2017), 'In Vietnam and across Asia, hard lessons for ransomware victims', *Vnexpress*. Retrieved from: https://e.vnexpress.net/news/news/in-vietnam-and-across-asia-hard-lessons-for-ransomware-victims-3585383.html [accessed 30 November 2023]

[69] Rothwell D. R., Kaye S., Akhtarkhavari A., and Davis R. (2010), 'Jurisdiction', in *International Law: Cases and Materials with Australian Perspectives*, Cambridge University Press

[70] Rosenberg D. (2022), 'Seizing the means of disruption: international jurisdiction and human rights in the expanding frontier of cyberspace', *International Law and Politics*, Vol. 55

[71] Security Council (2021), 'Explosive' Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats', SC/14563, 29 June 2021

[72] Semenova N. (2021), 'Jurisdiction in Cyberspace'. Retrieved from: http://dx.doi.org/10.2139/ssrn.3912006 [accessed 30 November 2023]

[73] Sénat (2020), 'Rapport d'information n° 613 (2019-2020)', *Proposition de résolution au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, sur la lutte contre la cybercriminalité : Cybercriminalité : un défi à relever aux niveaux national et européen*, 9 July 2020

[74] Schmitt M. (2021), 'The Sixth United Nations GGE and International Law in Cyberspace', *Just Security*. Retrieved from: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/ [accessed 5 December 2023]

[75] Schmitt M. N., Vihul L. (2017), 'Respect for Sovereignty in Cyberspace', *Texas Law Review,* Vol. 95, No. 3

[76] Statista Research Department (2023), 'Global ICT market share 2013-2023, by selected country'. Retrieved from: https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/#:~:text=As%20of%202023%2C%20the%20U.S.,share%20of%20over%2011%20percent [accessed 17 December 2023]

[77] Tan E. E., Ang B. (2022), 'ASEAN Ambiguity on International Law and Norms for Cyberspace', *Baltic Yearbook of International Law Online*, Vol. 20, Issue 1

[78] Tay K. L. (2023), 'ASEAN Cyber-security Cooperation: Towards a Regional Emergency- response Framework', *The International Institute for Strategic Studies*

[79] The European Commission (2022), 'The Cybersecurity Strategy'. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy [accessed 5 December 2023]

[80] The European Commission (2022), 'Joint Communication to the European Parliament and the Council', *the EU's Cybersecurity Strategy for the Digital Decades*

[81] The Information Office of the State Council of the People's Republic of China (2010), 'The Internet in China', *Information Office of the State Council of the People's Republic of China*. Retrieved from: http://www.china.org.cn/government/whitepaper/node_7093508.htm, pp. 7-8 [accessed 17 December 2023]

[82] The NATO Cooperative Cyber Defence Centre of Excellence (2023), 'The Tallinn Manual', *CCDCOE*. Retrieved from https://ccdcoe.org/research/tallinn-manual/ [accessed 6 December 2023]

[83] The United Nations (2021), 'Ransomware attacks, a growing threat that needs to be countered', *UNODC Regional Office for Southeast Asia and the Pacific*

[84] The UN Secretary-General (2013), 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', *U.N. Doc. A/68/98*, 24 June 2013

[85] Trachtman J. P. (1998), 'Cyberspace, Sovereignty, Jurisdiction and Modernism', *Indiana Journal of Global Legal Studies*, Vol. 5, No. 2

[86] United Nations Office on Drugs and Crime (2019), 'E4J University Module Series: Cybercrime - Module 7: International Cooperation against Cybercrime'. Retrieved from https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html [accessed 5 December 2023]

[87] Van Ly (2018), 'Quốc hội: Hợp nhất luật an ninh mạng và an toàn thông tin là không khả thi' [trans: Congress: Consolidating cybersecurity and information security laws is not feasible], *The Saigon Times*. Retrieved from: https://thesaigontimes.vn/quoc-hoi-hop-nhat-luat-an-ninh-mang-va-an-toan-thong-tin-la-khong-kha-thi/ [accessed 5 December 2023]

[88] Vietnam's Government, 'Report on the activities of mutual legal assistance in 2019', No. 479/BC-CP, 12 October 2019. Retrieved from https://congan.com.vn/tin-chinh/thu-thap-chung-cu-ve-hanh-vi-gui-tien-qua-lao-va-campuchia-cua-tran-bac-ha_81536.html [accessed 30 November 2023]

[89] Vietnamplus (2022), 'Vietnam asks for EU's stronger support in cyber security protection', 28 April 2022. Retrieved from https://en.vietnamplus.vn/vietnam-asks-for-eus-stronger-support-in-cyber-security-protection/227696.vnp [accessed 5 December 2023]

[90] VnetWork (2023), 'Vietnam's cybersecurity in the first half of 2022', *VnetWork*. Retrieved from: https://www.vnetwork.vn/en-US/news/an-ninh-mang-viet-nam/11 [accessed 30 November 2023]

[91] Vu T. T. Anh (2023), 'Protecting Vietnam's Sovereignty in Cyberspace: Insights from Human Right Laws', *The Age of Human Rights Journal*, Vol. 21

[92] Vyas R. K. (2022), '3 Reasons Southeast Asia Is A Hot Market For Tech Startups', *Forbes*, 17 May 2022

[93] Wen R. (2019), 'Vietnam's New Cybersecurity Law: A Headache for US Service Providers?', *Georgetown Law Technology Review*. Retrieved from: https://georgetownlawtechreview.org/vietnams-new-cybersecurity-law-a-headache-for-us-service-providers/GLTR-02-2019/ [accessed 5 December 2023]

[94] Yang M. (2016), 'Legal Ambiguities in Cyberspace', *LawTech.Asia*. Retrieved from: https://lawtech.asia/legal-ambiguities-in-cyberspace/ [accessed 29 November 2023]

[95] Yiapanis A., Mazzola A. (2023), 'Opinion of the European Economic and Social Committee on the Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence', *Official Journal of the European Union*, 2023/C 293/04

[96] Zachar D. (2021), 'Battling Cybercrime Through the New Additional Protocol to the Budapest Convention', *The NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved from: https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/ [accessed 29 November 2023]

Author Contribution

The author solely contributed to the study conception and design. The author read and approved the final manuscript.

Declarations

Conflict of Interest: The author declares no competing interests.

Disclaimer: All claims expressed in this article are solely those of the author and do not necessarily represent those of the author's affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article or claim that may be made by its manufacturer is not guaranteed or endorsed by the publisher.