eudaimonia

Journal for Legal, Political and
Social Theory and Philosophy

Vol. 8 No. 1 • 2024.

Published by

IVR SERBIA

Journal for Legal, Political and
Social Theory and Philosophy

PROTECTING NATIONAL SOVEREIGNTY IN CYBERSPACE WITHIN THE CONTEXT OF DIGITAL GLOBALIZATION – REGULATIONS OF SOME COUNTRIES AND PROPOSALS

Trong Hiep Dinh
Phuong Chi Nguyen

Pages: 5–29

UDK 34/384.3
DOI 10.51204/IVRS_24101A

Trong Hiep Dinh*

Phuong Chi Nguyen**

PROTECTING NATIONAL SOVEREIGNTY IN CYBERSPACE WITHIN THE CONTEXT OF DIGITAL GLOBALIZATION – REGULATIONS OF SOME COUNTRIES AND PROPOSALS

The explosive growth of digital technologies is creating a virtual and borderless environment, which is so-called "cyberspace". In addition to serving as a platform that allows digital communication, information sharing, and online activities to take place, cyberspace carries various risks and vulnerabilities that can pose significant challenges to individuals, organizations, and even the nation. Throughout history, international law has built the concept of state sovereignty based on material aspects. However, digital globalization has significantly changed social relations, challenging important legal concepts that underlie international relations, including the concept of national sovereignty. Therefore, the issue of national sovereignty in cyberspace needs to be studied more carefully, thereby seeking appropriate solutions to protect national sovereignty in cyberspace.

Keywords: *Cyberspace Security, Digital Globalization, International law, National Law, National Sovereignty.*

1. INTRODUCTION

In June 2009, Robert Gates – the U.S. Secretary of Defense in an attempt to recommend the U.S. President to establish the U.S Cyber-Command (USCYBERCOM) as part of the U.S. Strategic Command (USSTRATCOM) has forecasted: "The next war will begin in cyberspace" (Army News Service 2009). This anticipation gradually becomes true as cyberspace security is currently one of the key agendas

* Research fellow at Hanoi Law University, tronghiepdinh153@gmail.com.

** Research fellow at Foreign Trade University, phuongchinguyen02@gmail.com.

in the Defense Policies of governments. In fact, there have been many cases where countries have become victims of cyber attacks. In 1982, a logic bomb was installed by the U.S. Central Intelligence Agency (CIA) into the computer system controlling the Soviet gas pipeline, causing a shocking explosion in Siberia (Heather Dinniss 2012, 6). In 2007, the homepages of the Estonian Government, banks, and television stations became a target of denial of service (DoS) attacks, resulting in removal of the original content (Marco Roscini 2012, 5). Notably, a computer worm called Stuxnet attacked Iran's industrial infrastructure in 2010 with the purpose of destroying centrifuges at the Natanz nuclear enrichment facility. Although the consequences of the incident have not yet been clearly announced, Iran had to temporarily suspend the uranium enrichment process at Natanz, according to the International Atomic Energy Organization (IAEA) (Broad 2010). The list of victims of cyber attacks will definitely continue to expand in the context of increasingly complicated international relations.

If the next war will indeed be in cyberspace, then what should the international community do about it? Having all this in mind, the authors decided on the topic "Protecting national sovereignty in cyberspace within the context of digital globalization – regulations of some countries and proposals" in order to analyze the above-mentioned issues more clearly and suggest some proposals for parties to secure the national security on cyberspace. The paper will clarify the following legal issues related to national sovereignty in cyberspace.

Firstly, the paper will analyze international law developments on cyberspace security. The international law on cyberspace security has undergone a long period of development and application since the 20th century when governments gradually realized the rapid advancement of information technology and widespread usage of the Internet. As a result, the issue of how cyberspace should be regulated has become a severe concern in countries worldwide. Accordingly, the paper will elucidate and analyze the process of developing international law on cyberspace security, including the process of analyzing, discussing among countries, and reaching an agreement on this issue. After analyzing the developments of international law on cyberspace security, the paper will clarify and analyze the importance of protecting sovereignty in cyberspace within the context of digital globalization.

Secondly, the paper will review the intricate landscape of regulations aimed at safeguarding national sovereignty in the realm of cyberspace. By examining the legal frameworks implemented by various countries around the world, the paper aims to shed light on the diverse approaches taken to address this pressing issue. In particular, we shall explore different strategies employed by different countries to secure their digital borders, mitigate cyber threats, and preserve their national interests.

Thirdly, the paper will analyze some contrasting views of countries on ensuring cyberspace security, in terms of policies, countermeasures, etc. After analyzing the international laws as well as domestic laws of countries, regarding the protection of sovereignty in cyberspace, the paper will point out and evaluate contrasting views that still exist between countries on this issue. These inadequacies arise in the process of exchange and negotiation processes aimed at improving the effectiveness of protecting the country's sovereignty in cyberspace. These contrasting views are part of the reason why the protection of the country's sovereignty in cyberspace is not yet effective and still appears to have shortcomings.

Fourthly, the paper will propose a range of solutions aimed at safeguarding governmental sovereignty in cyberspace. These solutions may encompass the development of robust cybersecurity frameworks, the establishment of international cooperation and information-sharing mechanisms, the implementation of effective legislative measures, and the nurturing of a skilled cybersecurity workforce. Through these proposed solutions, governments can aspire to preserve their sovereignty, ensuring the security, stability, and integrity of their digital domains.

2. THE DEVELOPMENT OF INTERNATIONAL LAW ON CYBERSPACE SECURITY

2.1. The development of international law on cyberspace security

Since the late 1990s, the United Nations (UN) has attempted to identify and assess the challenges that the digital revolution brings. Accordingly, the UN General Assembly has issued various annual Resolutions related to information security, affirming that "the spread and use of information technology and equipment can affect the interests of the entire international community" (Nguyen Tien Duc, Tran Thi Thu Thuy 2019), and "intentional misuse of these technologies could have dangerous implications for all nations" (Resolution No. 55/63/2000, UN General Assembly).[1] Deriving from this spirit, the UN General Assembly has endorsed the holding of the 1st World Summit on the Information Society. The Geneva Declaration of Principles and Geneva Plan of Action adopted at the Summit matched an important milestone when the international community made stipulations about the basic principles of internet-based information society and internet governance. Article 49 of the Declaration recognized the sovereign right of States for Internet-related public policy issues.[2]

Then, in 2004, the UN established the Group of Governmental Experts (GGE) on "Developments in the Field of Information and Telecommunications in the Context of International Security" in order to examine existing and potential threats arising from the use of Information and Communications Technologies by States, and considered actions to address them, including norms, rules, principles and confidence-building measures. In June 2013, the UN has published the third report of the Group, stating that "state sovereignty and international norms and principles that flow from sovereignty apply to state conduct of Information and Communications Technologies – related activities, and to their jurisdiction over Information and Communications Technologies infrastructure within their territory".[3] This statement of the GGE points out that application of state sovereignty is embodied in the following two levels: *First*, in a technical level, state sovereignty applies to Information and Communications Technologies infrastructure, which is located in the level of "cyber" including the internet, telecommunication networks and communication systems, communication systems and radio and television networks, computer systems, and embedded processors and controllers in key industrial facilities. *Second*, in a social level, state sovereignty applies to Information and Communications Technologies activities, which is located in the level of "space", that is, activity forms on the platform of Information and Communications Technologies system (Fang 2018, 80).

[1] UN General Assembly Resolution No. 55/63 of December 4, 2000.

[2] Geneva Declaration of Principles 2003, Paragraph a, Art. 49.

[3] UN General Assembly, 2013 UN GGE Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Article 20.

Besides the UN, international organizations also make efforts to research the impact of digital technology on international security and stability. One of the notable documents is the Budapest Convention on Cybercrime, signed in November 2001 and officially taking effect in 2004. Currently, this is the only binding international document relating to cybercrime acts. Accordingly, the Budapest Convention divides cybercrime into four groups: violations of the confidentiality, integrity and availability of computer data and computer systems; computer-related crimes; crime-related content; infringe copyright and neighboring rights. Also, each Party of the Convention shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held accountable for a criminal offense established in accordance with this Convention, committed for their benefit by any natural person (European Treaty Series – No. 185/ 2001; Council of Europe).[4]

Reputable jurists in the field of international law have also provided useful opinions and suggestions related to cyberspace security issues. In early 2017, Michael Schmitt published the document "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" (2017). The guide outlines how international law applies to cyber activities in peacetime and war conflicts, and analyzes common cyber incidents that countries face every day.

It is evident that the international community currently lacks a widely disseminated international document regulating cyberspace, cyber security and its related legal issues. Most countries are implementing their own cyberspace governance activities within their territories, maintaining benefits and limiting challenges from cyberspace. Negotiating on an international document related to this issue is considered too soon for some countries due to disputes over the interests and obligations of the parties. As such, states currently claim to rely on the principles of the UN Charter and other relevant documents in resolving issues related to cyberspace security.

2.2. The importance of protecting national sovereignty in cyberspace within the context of digital globalization

The rapid development of the Internet has revolutionized the functioning of nations and societies, driving economic progress, facilitating communication, and fostering innovation. However, with these

[4] Convention on Cybercrime, section 1, Council of Europe, *European Treaty Series* No. 185/2001.

advancements come inherent challenges, particularly in maintaining national sovereignty in cyberspace. Since countries become increasingly interconnected, the significance of protecting national sovereignty in cyberspace cannot be overstated.

First, national sovereignty is the cornerstone of a nation's identity, enabling countries to have the right to govern their internal affairs without external interference, contributing to peace and stability in international relations. National sovereignty serves as the foundation for international cooperation and provides the legal framework for treaties and agreements. Therefore, respecting and protecting national sovereignty is always the utmost priority for countries to maintain the autonomy and rights of individual nations within the global community.

Second, the nature of cyberspace allows information to flow freely, regardless of geographical boundaries, creating an interconnected and expansive domain. This borderless nature exposes inherent risks, as cyber threats can emerge from any corner of the globe, rapidly crossing national borders and attacking national sovereignty. Cyberspace has become a new battleground for both state-sponsored and non-state actors. Without adequate protection, national sovereignty can be compromised, leaving governments vulnerable to cyberattacks, data breaches, and malicious interference. Several recorded instances during the past decade have demonstrated the vulnerability of nations to cyber attacks. Numerous countries, including Kyrgyzstan, South Korea, Switzerland, England, and the U.S, have also reported being victims of cyber attacks. With the complexity of international relations increasing, it is expected that the list of cyber attack victims will continue to expand. Hence, the protection of national sovereignty in the digital realm plays an important role in safeguarding a nation's critical infrastructure, such as power grids, transportation systems, and communication networks. The integrity of these systems is paramount, as any breaches can result in severe consequences, including the disruption of essential services and compromising national security. By upholding sovereignty, governments can implement robust cybersecurity measures and effectively counter cyber threats arising from both domestic and international origins.

Third, preserving national sovereignty in cyberspace enables countries to design and implement policies that effectively and properly adapt to their own needs and circumstances. It grants countries the ability to navigate the ever-changing digital landscape, create regulatory frameworks, and devise national strategies concerning cybersecurity, digital infrastructure growth, and technological advancement. By safeguarding sovereignty, countries can assert their control over the digital domain, guaranteeing that decisions made align with the welfare and interests of their own government and citizens.

Fourth, during the period of international economic integration, the economies heavily depend on interconnected networks and digital platforms. As a result, preserving national sovereignty in cyberspace plays a crucial role in ensuring a nation's economic stability. Governments must have the authority and capacity to regulate and safeguard their digital markets, intellectual property, and other sensitive economic data/assets. Without well-protecting sovereignty, countries face the risk of relinquishing control over their economic resources, making them vulnerable to economic espionage and unfair competition. By protecting sovereignty, governments can ensure fair and secure digital trade, promote domestic industries, and foster innovation to drive economic growth.

Fifth, cyberspace has become a global platform where ideas, values, and cultural expressions are freely exchanged. Therefore, protecting national sovereignty in cyberspace allows governments to preserve their cultural identity and protect their citizens' cultural values. Nations have the right to govern and control the content and information circulating within their borders to ensure that it aligns with their cultural and societal norms. This not only serves to preserve their cultural heritage but also contributes to maintaining security, political stability, and safeguarding national interests. By exercising sovereignty in cyberspace, governments can effectively manage the digital realm in a manner that respects their culture and preserves their socio-political fabric.

As stated in the introduction, Robert Gates' forecast of "The next war will begin in cyberspace" cannot be more accurate at the present time. This encourages countries to enhance their awareness of the importance of cyber sovereignty and, at the same time, requires them to invest appropriate resources in protecting cyber sovereignty as they have traditionally done in military competition.

3. DIFFERENT APPROACHES OF COUNTRIES ON THE PROTECTION OF CYBERSPACE SOVEREIGNTY

It is widely acknowledged that international law concepts, including the fundamental principles of sovereignty and non-intervention, are considered applicable to the actions of states in cyberspace (Harriet Moynihan 2019). However, the practical application of these principles and their interpretation by different countries remain the subject of ongoing debate. The absence of a consensus on how international law should be applied to states' cyber activities has resulted in legal ambiguity and triggered many jurisdictions to establish their own framework to protect national security and sovereignty.

In this regard, States will normally exercise their sovereign powers by controlling and regulating cyberinfrastructure in their territory exclusively and independently. Some states choose to regulate certain aspects of cyber activity in their territory, for example, through laws about the processing of personal data and permissible content on the internet, while others exert tighter controls over access to the internet and personal data. This paper will then discover different strategies employed by different legislations to secure their digital borders, mitigate cyber threats, and preserve their national interests.

3.1. The legal frameworks on cyberspace sovereignty implemented by some countries in the world

3.1.1. The United States

The United States (U.S.) have asserted that sovereignty is only a principle rooted in international law, and therefore, no regulations or guidelines need to be derived from this principle that would be applicable specifically to cyberspace (Harriet Moynihan 2019). Unlike the conventional framework of sovereignty, which encompasses territorial, aerial, and maritime domains where States assert their power through domestic laws, the internet or cyberspace, in its entirety, appears to transcend physical limitations. It only functions as a virtual network connecting nodes, lacking a tangible existence that can be constrained by geographic or physical boundaries, thus challenging the notion of territorial sovereignty or control by any particular state (Adams, Jackson, Mohamad Albakajai 2016).

The U.S. has a long history of taking a relatively hands-off approach to cyberspace regulation compared to some other countries. While there are laws and regulations related to cybersecurity and data protection, such as the Computer Fraud and Abuse Act, the Federal Information Security Management Act, or The Federal Trade Commission Act, these do not touch much on the sovereignty aspects, giving room to promote a free and open internet. Some explain the reason behind this is that the early designers and developers of internet technology had a political desire to satisfy the wishes of the capitalists in the U.S. (James Lewis 2010, 55–65). Which, the primary purpose was to limit the governmental powers by establishing a globally accessible network that operates without a central command node, promoting a stateless and open connection across the world (Gary Schneider 2013). The view that cyberspace is a Global Commons, thereby falling outside the jurisdiction of any specific country, is reiterated scatter in various official documents of the U.S. government, as well as in statements made by non-governmental organizations (NGOs) operating within the country. Specifically, in the 2018 National Defense Strategy (Association of the U.S. Army 2008), the U.S. Secretary of Defense only set out their Domain Preeminence over the land, air, and sea, while putting the data transmitted via sea or air in the discussion of global commons. In the 2018 National Cyber Strategy, President Donald J. Trump repeatedly used the term "global" when discussing the nature of cyberspace. Some scholars did support such view, by proving that (i) the IP address, a unique numerical identifier assigned to devices connected to a computer network; (ii) the DNS, a decentralized naming system that translates human-readable domain names; and (iii) the cyberspace and the connection therein are the common resources brought out by the Internet, but not by any specific government. In terms of the NGO's viewpoints, A Declaration of the Independence of Cyberspace by John Perry Barlow, the founder of Electronic Frontier Foundation (EFF), is a notable statement. The EFF is a non-profit organization based in the U.S. that champions civil liberties and digital rights in the realm of technology. In the Declaration, John asserts that the governments have no sovereignty over cyberspace, which he called "the new home of Mind," and "the global social space people are building to be naturally independent of the tyrannies the government seek to impose on" (John Barlow 1996).

However, the above does not mean that the U.S. has given up its right to claim sovereignty in cyberspace. On the contrary, as cyber attacks on government organizations are increasing, the country has been more focused on protecting critical infrastructure from cyber threats and addressing issues such as misinformation and cybercrime. Increasingly, senior the U.S. government officials have acknowledged this duty with respect to activities in cyberspace. In 2012, State Department Legal Adviser Harold Koh offered the first major statement on this matter, emphasizing that "States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict. The physical infrastructure that supports the Internet and cyber activities is generally located in a sovereign territory and subject to the jurisdiction of the territorial State. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered" (Harold Koh 2012). From a military perspective, General Keith Alexander – former Director of the U.S. National Security Agency, and the first commander of the USCYBERCOM said that the cyber sovereignty concept must serve a strategic goal of ensuring the freedom of action of the U.S. and its allies in cyberspace and denying the same rights to adversaries (Cynthia Ayers 2016). In later years, USCYBERCOM also declared that the U.S. will treat cyber attacks in the same manner as conventional attacks, and will exercise the interceptive self-defense rights as stipulated under Article 51 of the UN Charter, and even the anticipatory and preemptive self-defense, to best protect the States' interest (Geoffrey S. DeWeese 2015).

3.1.2. The United Kingdom

Situated in a distant geographical location, the United Kingdom (U.K.) somehow shares the same approach to cyber sovereignty as the U.S. The U.K. has long been known to possess a significant level of expertise and influence in the application of international law to the realm of cyberspace. A noteworthy development, however, was first witnessed in 2018 during a discourse delivered by the former Attorney General, Jeremy Wright, at the esteemed Chatham House. Surprisingly, Wright expressed an unconventional standpoint by rejecting the existence of a governing principle of sovereignty applicable to cyber operations. The U.K. maintains that while sovereignty is a fundamental principle in international law, it does not provide a sufficient or clear basis for establishing specific rules or additional prohibitions for cyber conduct, and asserts that relying solely on the broad concept of sovereignty is insufficient for developing a comprehensive framework that effectively governs cyber operations beyond the principle of non-intervention (Michael Schmitt 2022). By adopting this viewpoint, the U.K. maintains that the prohibition on intervening in the internal or external affairs of other states serves as the fundamental criterion for evaluating acts of internationally wrongful conduct in the majority of cyber operations conducted remotely. This position allows the U.K. to conduct cyber operations in another state's territory without violating sovereignty, as long as it does not exceed the boundaries of non-intervention.

After such controversial speech, the U.K. subsequently issued two additional statements pertaining to the role of international law in cyberspace. These include a declaration made in 2021 for the UN GGE on cyberspace and a speech delivered in May 2022 by the current U.K Attorney General, Suella Braverman, at Chatham House. While there have been limited changes in the U.K.'s stance since 2018, each statement has contributed to a more detailed delineation of the U.K.'s positions on this matter. Specifically, the 2021 UN GGE statement by the U.K., reiterated the U.K.'s position on sovereignty, while none of its NATO allies, including the U.S., followed suit. The statement acknowledged the existence of differing opinions on sovereignty but emphasized that such differences should not hinder states from evaluating whether specific situations constitute internationally wrongful acts and reaching common understandings on those matters. Regarding the application of the UN Charter, the statement recognized that the prohibition on the use of force and the right to self-defense in response to an armed attack also extend to the cyber domain. However, it did not explicitly address whether cyber operations that are non-destructive or non-injurious could be considered as a use of force or an armed attack. Instead, it suggested that if cyber operations produce effects similar to those caused by kinetic actions that qualify as a use of force or an armed attack, they would be treated likewise. Following by GGE reports, Attorney General Suella Braverman reiterated the U.K.'s stance on non-intervention and discussed the concept of coercion and collective measures in cyber operations in her speech before Chatham House in 2022. The Attorney General emphasized that states should not coercively interfere in the affairs of others. Coercion was thereby defined as depriving a state of control over its "domaine réservé", which refers to areas where international law allows states to make decisions freely, and cyber operations disrupting this control were deemed unlawful. The speech acknowledged the evolving definition of coercion and the ongoing debate on collective countermeasures, without taking a firm stance. In general, the U.K. aligns with mainstream views on how international law applies to cyberspace, except for its stance on sovereignty. However, as more states adopt a different perspective and the U.K. is likely to seek common in defining unlawful cyber operations, the significance of this disagreement is diminishing rapidly (Michael Schmitt 2022).

3.1.3. Russia

Russian leaders perceive cyberspace as a critical arena in the global power struggle, attributing special significance to it in terms of Russia's power and influence internationally. Consequently, Russia adopts a proactive stance on cyberspace sovereignty, positioning itself as being "one step ahead" in this field. In the context of "Russia is facing cyber threats of a military, criminal, and terrorist nature, the most serious challenge to national security and international peace in the 21st century", as said by President Putin when signing a pact to create communication link on cyber security with the U.S. (Ellen Nakashima 2013), Russia is currently starting to build a concept of "cyberspace sovereignty" based on the sovereignty concept of the Russian Military Encyclopedia. Accordingly, these concept involves granting Russia powers to (i) exert control over the realms of "cyber engineering" and "cyberpsychology", which together constitute the two distinct aspects of cyber warfare; (ii) gain an advantage over adversaries and safeguard vital national assets by exercising control over devices in the realm of cybersecurity; (iii) exercise authority over the national cyberinfrastructure; and (iv) censor and manage the information in cyberspace (Digital and Cyberspace Policy Program and Net Politics 2020).

Russia has concretized its view on cyber sovereignty by implementing several domestic laws and regulations, including, but are not limited to: (i) Data Localization Law (2015), which requires personal data of Russian citizens collected by both domestic and foreign companies to be stored within the territory of Russia and grants Russian authorities access to such information; (ii) Federal Law on Counteracting Terrorism (2016), which mandates telecommunications operators and internet service providers to retain user data for specified periods and provide access to security agencies upon request and requires encryption keys to be provided to authorities, which can have implications for user privacy and data security; (iii) Sovereign Internet Law (2019), which provides the Russian government with extensive control over the internet within its borders and grants Russian authorities the power to regulate and potentially isolate the Russian segment of the internet (Runet) in case of perceived external threats or emergencies, (iv) Information Security Law (2006, amended in 2019), which establishes a legal framework for information security and aims to protect critical information infrastructure within Russia and prevent cyber threats. For the most recent development, in 2019, Russian President Vladimir Putin approved a law requiring that all smartphones, computers, and smart TV sets sold in Russia must be equipped with pre-installed Russian software, which later came into force in July 2020. Also, in 2018, Russia also proactively put forward a resolution at the UN General Assembly, allowing legitimized state surveillance and censorship through its emphasis on sovereignty and non-interference in the internal affairs of countries. The resolution created an Open-ended Working Group (OEWG) on the topic of cybersecurity to run parallel to the already existing UN GGE, effectively bifurcating the discussion of cyber norms at the UN. This could allow Russia to use the OEWG as a forum to reinterpret previous UN GGE reports to better align with Russian preferences for internet governance. Within internet governance, Russia has enacted measures to impede access to select websites and control online content deemed to contravene Russian legislation or pose a risk to national security. The government possesses the capability to direct internet service providers to block access to particular web addresses or even entire platforms. Russia also maintains stringent regulations governing online content, granting the government the authority to prohibit websites and social media platforms that are perceived to disseminate illicit or detrimental information. The above efforts have clearly demonstrated Russia's views on cyberspace sovereignty.

3.1.4. China

Echoing with its neighbor Russia, on this matter, China is well-known for having strict regulations on cyberspace. Since 2013, cyber security has become one of the most important issues on the agenda of the Grand National Security strategy, especially after the founding of a new Working Group on Cyber Security and ICT, which directly led President Xi Jinping to meet the challenges and threats rising within cyberspace (Shen Yi 2014, 41– 43). Since then, President Xi and the Chinese government have set a major goal for China in cyberspace, which is to transform China into a cyber power where increasing not only effectively defends against potential cyber threats but also China influences shaping the global rules governing cyberspace (Cyberspace Administration of China 2015). However, in his speech to China's Second World Internet Conference in 2015, President Xi called on countries to respect each other's cyberspace sovereignty and different governance models, and no country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security" (Xi Jinping 2015). In 2016, Chinese Ambassador Liu Xiaoqing, speaking at the "Cyber 2016" Conference held in the U.K, also proposed that the concept of "equal sovereignty" enshrined in the UN charter should also be applied to cyberspace. These statements somehow reflect the understanding of the Chinese government of the concept of cyber sovereignty, which includes key components: (i) it emphasizes the state's authority to control the flow of information within its territory; (ii) it recognizes that each state has the autonomy to formulate its own policies regarding cyberspace; (iii) it highlights the principle that all states should have equitable participation in shaping the rules, norms, and code of conduct governing the global cyberspace and (iv) it underscores the significance of respecting sovereignty as a fundamental guiding principle in addressing international cyber-related matters (Xinhua Net 2014).

In light of the above, China has implemented several laws and regulations related to cyber sovereignty, some highlighted regulations can be named as (i) Cybersecurity Law implemented in 2017, which establishes the legal framework for safeguarding China's cyberspace sovereignty and requires network operators to ensure the security of their networks, protect user information, and cooperate with government authorities in matters related to cybersecurity; (ii) National Intelligence Law, enacted in 2017, which empowers Chinese intelligence agencies to gather intelligence on threats to national security, which includes information and communication systems; and specifically, (iii) National Security Law of China enacted in 2015, which clearly sets out the protection of sovereignty in cyberspace is one of the tasks of ensuring national security. These legal instruments refers to the state's control and governance over the internet within its borders. Therefore, they aim to regulate online activities, safeguard national security, protect the rights of citizens, and promote Chinese values and interests in the digital realm. Besides, in support to such regulations, the country also operates a sophisticated system of internet censorship and content filtering known as the Great Firewall of China, employing various technical measures to block access to foreign websites and content deemed undesirable or politically sensitive. According to Ankit Kumar (2023), the Great Firewall is aimed at maintaining control over information flow and preventing the dissemination of content that could challenge the Chinese Communist Party's authority. Similar to Russia, China also imposes data localization mandates, which dictate that personal and significant data obtained within China's borders must be stored and managed on domestic servers, adhering to Chinese regulations and supervision. It should be noted there are several debates and criticism from international observers who argue that China is restricting freedom of expression, and privacy rights, and hinders open access to information, yet the Chinese government maintains its stance that these measures are necessary for national security and social stability.

3.1.5. South East Asia

Cybersecurity is a key enabler of the economic progress and betterment of living standards in the digital economy for Association of Southeast Asian Nations (ASEAN) countries. This has become even more apparent during and after the Covid-19 pandemic, which witnessed a rapid shift towards digitalization and the widespread migration of government, business, and social activities to online platforms. Given this trend, ASEAN countries altogether published a draft of the ASEAN Cybersecurity Cooperation Strategy for the years 2021–2025, which emphasizes the importance of cybersecurity in supporting the economic progress and well-being of ASEAN member states in the digital economy. The proposed strategy aims to ensure the security and stability of cyberspace through five dimensions of work, including (i) advancing cyber readiness cooperation, (ii) strengthening regional cyber policy coordination, (iii) enhancing trust in cyberspace, (iv) regional capacity building and (v) international cooperation. The draft also mentions the establishment of an ASEAN Cybersecurity

Coordinating Committee and the development of an ASEAN Computer Emergency Response Team (CERT) to enhance incident response capabilities. While waiting for the official publication of this strategy and other mutual agreements, individual ASEAN member states have their own national laws and regulations pertaining to cyberspace and cybersecurity. These laws may address various aspects such as data protection, online privacy, cybersecurity standards, cybercrime prevention, and digital governance.

In Vietnam, since 2021, the State has announced that sovereignty over cyberspace is an important part of national sovereignty, and ensuring sovereignty in cyberspace helps to protect national sovereignty (Vietnam News 2021). Speaking at the national scientific conference on "Ensuring national sovereignty in cyberspace", Associate Professor, Dr. Nguyễn Văn Thành, special Vice Chairman of the Central Theoretical Council, former Deputy Minister of Public Security, said that national sovereignty in cyberspace is a supreme, absolute and complete right (Vietnam News 2021). It is the responsibility of the State to exercise direct or indirect management and control over cyberspace through the implementation of policies, laws, and technological capabilities, which must be carried out in accordance with international laws and regulations. Within its own jurisdiction, Vietnam has set out its own legal framework on cyber security and cyber sovereignty, including (i) the Law on Cybersecurity, passed in 2018,[5] and (ii) Decree on Data Privacy, passed in 2023,[6] which grants authorities broad powers to monitor, control, and regulate online activities. These laws require service providers to store user data within Vietnam's territory and cooperate with government agencies in matters related to cybersecurity and information control. The Vietnamese government has also established specialized agencies and units, such as the Ministry of Public Security's Department of Cybersecurity and High-Tech Crime Prevention (A05), to enforce cybersecurity measures, combat cyber threats, and monitor online content.

Malaysia, like many other countries, acknowledges the significance of cyber sovereignty and has articulated its perspective on the subject. The Malaysian government underscores the necessity of retaining authority and overseeing cyberspace within its territorial boundaries to safeguard national security, uphold the integrity of its political system, and maintain social cohesion. Malaysia's approach to

[5] Law on Cyber security (Vietnam) No. 24/2018/QH14.

[6] Decree on Data Privacy (Vietnam) No. 13/2023/ND-CP.

cyber sovereignty involves enacting laws, regulations, and policies to govern and safeguard its cyberspace. The country has implemented (i) the Personal Data Protection Act to regulate the collection, use, and disclosure of personal data by organizations,[7] along with (ii) the Communications and Multimedia Act empowers the government to regulate and oversee the telecommunications and multimedia sectors, including online content and electronic transactions.[8] The Malaysian government also focuses on cybersecurity and has established agencies such as the National Cyber Security Agency (NACSA) to coordinate and enhance the country's cybersecurity efforts, aiming to protect critical information infrastructure and combat cyber threats. However, it is worth noting that Malaysia adopts an inclusive and balanced approach to governing cyberspace. On the one hand, the Malaysian government recognizes the significance of digital innovation, economic advancement, and the freedom of expression in the online realm, especially via developing an internal infrastructure known as the Multimedia Super Corridor (Toby E. Huff 2001, 439–458), which encompasses both a physical location and an electronic "cyberspace" aimed at promoting the growth of the information and communication technology industry in Malaysia. On the other hand, it also emphasizes that individuals and organizations have a responsibility to adhere to the laws and regulations in place to uphold cybersecurity and safeguard the overall welfare of the country.

Thailand has expressed its views on cyber sovereignty, emphasizing the need for government control and regulation over cyberspace to ensure national security, protect its political system, and maintain social order. Thailand has enacted various laws and regulations to exercise control over cyberspace and maintain cyber sovereignty, including (i) the Computer Crime Act and (ii) the Cybersecurity Act, which empower the government to regulate and monitor online activities, combat cyber threats, and protect critical information infrastructure. Similar to Vietnam and Malaysia, the Thai government has also established agencies such as the National Cybersecurity Committee, the NACSA, and the Electronic Transactions Development Agency to oversee and coordinate cybersecurity efforts. Online platforms and websites have been subject to government censorship and monitoring, and individuals have faced legal consequences for online activities deemed threats to national security or social order.

[7] Act 709 on Personal Data Protection 2010 (Malaysia).

[8] Act 589 on Communications and Multimedia 1998 (Malaysia).

3.2. The contrasting views of countries on ensuring the security in cyberspace

The development of international law pertaining to the seas has been a lengthy process spanning several decades, primarily due to varying perspectives and conflicting interests among maritime nations. Similarly, in the present day, countries continue to hold divergent views on the establishment of an international legal framework for ensuring national sovereignty and security in cyberspace.

According to the Permanent Delegation of the Socialist Republic of Vietnam in New York – the U.S. (2020), during the "Arria formula" meetings at the UN, countries have acknowledged the relevance of international law in addressing the use of information and communication technology. However, each country holds distinct positions on this matter. Australia and Japan, for instance, oppose the establishment of new rules and prioritize further discussions on the application of existing international law to cyberspace. Besides, the Ministry of Information and Communications of Vietnam (2023) points out that many Western countries currently do not support the development of new rules of international law in cyberspace. Among the existing rules, Western countries pay special attention to promoting the application of rules on responsible state behavior in cyberspace. Denmark and Nordic countries have emphasized that cyberattacks targeting critical infrastructure of other nations violate international law and norms of responsible state behavior. They strongly condemn such actions as "unacceptable". Also in this report, the U.S, the European Union, and Australia have highlighted the importance of state obligations to prevent malicious cyber activities from taking place within their borders in their respective statements. This aligns with the principles outlined in norms regarding responsible state behavior in cyberspace. Western countries also express their support for the "Action Program to promote responsible state behavior in cyberspace" put forward by France and Egypt, emphasizing the need for cooperation mechanisms (the Ministry of Information and Communications of Vietnam 2023).

In contrast, countries like China and Russia hold the view that new rules are necessary, reported from Allison Pytlak (2023). China, in particular, emphasizes the importance of broad participation in the formulation of new rules, with a specific focus on safeguarding the interests of developing nations. Among the existing rules of international law, China highlights the significance of complying with the UN Charter and other principles of international law. They stress the need to prevent the "battlefieldification" of cyberspace in order to protect critical infrastructure. China advocates for adherence to principles such as sovereign equality, refraining from the use or threat of force, peaceful dispute resolution, and maintaining the peaceful nature of cyberspace.

Meanwhile, Russia argues that the application of existing rules to cyberspace predominantly serves the interests of powerful nations, thereby perpetuating the injustices present in the physical world. As a result, they advocate for the adoption of a new universal and legally binding convention that would address the perceived Western-centric nature of the current Internet. Russia specifically mentions a document it co-submitted to the UN on an updated version of the International Information Security Treaty.

In addition to the contrasting positions of the major factions, other countries expressed their concerns with varying perspectives in their statements. According to Allison Pytlak (2023), Qatar and Pakistan, for example, mentioned the need for the development of new rules in cyberspace. However, they emphasized that these new rules should be legally binding and take into account the consequences of violating them. Developing countries, especially those with limited cyber capabilities, view binding international rules as a more dependable safeguard. They believe that such rules provide a stronger guarantee for their interests and security in the cyber domain. Mozambique, rather than proposing new rules, highlighted the need to reassess the concept of cyber sovereignty, emphasizing that the existing capacity asymmetries in the physical world should not be replicated in cyberspace. This viewpoint aligns with Russia's perspective. Furthermore, Albania, Latvia, Brazil, and Pakistan utilized the occasion to appeal to the international community for support in enhancing network capacity in developing countries (the Security Council 2023). These countries recognize the significance of bridging the digital divide and ensuring that developing nations have the necessary resources to improve their cyber capabilities and participate more effectively in the digital realm.

Indeed, the aforementioned perspectives of various countries demonstrate the existence of divergent "factions" in the realm of international law in cyberspace. These differences in perspectives and conflicts of interest have contributed to the conflicting views during the process of establishing an international legal framework for ensuring security in cyberspace. The complex nature of cyberspace, coupled with the diverse interests and concerns of different countries, present significant challenges in reaching a consensus on such a document. However, recognizing the importance of global cooperation and addressing the unique challenges of cyberspace is crucial for promoting stability, security, and the protection of rights and interests in the digital domain. Also, efforts to bridge the gaps and foster dialogue among nations are very important for advancing the development of an effective and inclusive international legal framework for cyberspace.

4. SOLUTIONS FOR COUNTRIES FOR SAFEGUARDING GOVERNMENTAL SOVEREIGNTY IN CYBERSPACE

4.1. Constructing international cooperation on cybersecurity

Without a doubt, enhancing the function of international organisations, enhancing the global network management system, and jointly ensuring network security are essential to promoting cooperation in cyberspace. Countries ought to work together more in fields of technical cooperation, combating cyberterrorism and cybercrime, and strengthening the Internet's multilateral, democratic, and open governance. This would progressively create a system in which cyberspace would become both beneficial to all nations and a fundamental component of cooperation.

Mutual respect, trust, equality, and benefit-sharing are essential for strengthening international cooperation and collaboration to confront emerging risks and difficulties. Organisations like the UN, the Shanghai Cooperation Organisation, the International Telecommunication Union, the BRIC countries, and the ASEAN Regional Forum are good places for nations to collaborate. These platforms have the potential to enhance national cooperation, foster peaceful dispute resolution, foster the establishment of international information security legal norms, and enable cooperation.

Coordination among relevant international organizations is also essential to ensure effective collaboration and address the complex and evolving landscape of cybersecurity. By strengthening these efforts, countries can promote greater cooperation, enhance security, and foster the sustainable development of cyberspace.

4.2. Enhance national capacity in ensuring security in cyberspace

Proactive steps are needed to prevent information technology misuse that could jeopardise international security and stability in order to create a "peaceful" cyberspace. It is imperative that we all refuse participating in an arms race in cyberspace and work to stop conflicts there. Rather, the emphasis ought to be on utilising cyberspace in a way that is consistent with humanity's shared interests. The UN Charter's tenets, which forbid using or threatening to use force, should be upheld by all states. This dedication contributes to effectively reducing the misuse of technology and averting disputes in cyberspace. Countries may help create a safe and secure cyberspace that benefits all people by adhering to these principles.

Thus, safeguarding cyberspace sovereignty entails putting in place strong policies that complement a nation's stature in the world and its network capacities. It comprises building robust defence and security mechanisms for networks, quickly identifying and thwarting network intrusions, and guaranteeing a strong basis for national network security. Building a network border through cooperation between military and civilian groups is both an immediate challenge for countries' digital sovereignty and a long-term cornerstone for maintaining it, much as geographical sovereignty requires strengthened defences. Building a strong cyberspace sovereign security capability requires the combination of military and civilian resources. This strategy acknowledges that the only way to successfully handle the difficulties associated with cyberspace security is through military and civilian collaboration. Measures such as military-civilian integration, dual-use technologies, and joint efforts are necessary to establish a coordinated cyberspace sovereign security force.

4.3. Develop the level of cybersecurity education for all walks of life

Improving cybersecurity education is essential to enhancing cyberspace security as a whole. Strengthening a few important areas can help accomplish this. First and foremost, it is critical to raise public awareness of cybersecurity issues by teaching people about typical dangers and offering advice on safeguarding personal data. Additionally, incorporating cybersecurity education into curricula and programmes in schools can help cultivate a cybersecurity culture from a young age. Resources and training should be provided to educators so they can impart cybersecurity principles to students. Thirdly, in order to create a workforce with the necessary skills to tackle changing threats, it is imperative that cybersecurity education be improved for both professionals and current employees. This covers possibilities for ongoing professional growth, certifications, and specialised training programmes. Fourthly, targeted cybersecurity education and support programs for small and medium-sized enterprises (SMEs) can help them understand and mitigate risks. Additionally, cybersecurity education should target government officials and policy makers to enhance their understanding of cybersecurity issues. Lastly, promoting international cooperation and collaboration in cybersecurity education can facilitate knowledge sharing and capacity building among countries. By improving cybersecurity education in these areas, individuals, organizations, and nations can develop a strong cybersecurity awareness and expertise, contributing to a safer and more secure cyberspace for everyone.

5. CONCLUSION

In conclusion, as the world becomes increasingly interconnected and dependent on cyberspace, the protection of national sovereignty in this domain is of utmost importance. The potential for cyber warfare and the threats posed by malicious actors necessitate the development of effective governance and regulations. To secure national security in cyberspace, it is essential for countries to establish comprehensive legal frameworks that define the rights, responsibilities, and boundaries of states in cyberspace. These frameworks should address issues such as attribution of cyberattacks, the use of offensive cyber capabilities, and the protection of critical infrastructure. Furthermore, international cooperation and collaboration are vital in addressing the challenges of cyberspace. Countries should work together to develop common norms, standards, and principles that promote responsible state behavior in cyberspace. This includes fostering transparency, accountability, and trust among nations. At the same time, it is necessary to strike a balance between protecting national sovereignty and promoting digital globalization. Countries should avoid excessive restrictions that hinder the free flow of information and innovation, while ensuring that cybersecurity measures are in place to safeguard national interests. Most importantly, by working together and implementing effective measures, countries can safeguard their national security while promoting the benefits of digital globalization.

REFERENCE LIST

1. Adams, Jackson, Mohamad Albakajai. 2016. Cyberspace, A New Threat to the Sovereignty of the State. *https://core.ac.uk/reader/146502700* (last visited October 20, 2023).
2. Army News Service. 2009. Next war will begin in cyberspace, experts predict. *https://www.army.mil/article/17561/next_war_will_begin_in_cyberspace_experts_predict* (last visited 31 August, 2023).
3. Association of Southeast Asian Nations (ASEAN). 2021. Asean Cybersecurity Cooperation Strategy (2021–2025). *https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021–2025_final-23–0122.pdf* (last visited November 5, 2023).
4. Association of the U.S Army. 2008. The 2008 National Defense Strategy: Implications for the U.S Army. *https://www.ausa.org/sites/default/files/TBIP-2008-The-2008-National-Defense-Strategy-Implications-for-the-United-States-Army.pdf* (last visited October 20, 2023).
5. Ayers, Cynthia E. 2016. Rethinking Sovereignty in the Context of Cyberspace. *https://media.defense.gov/2023/Oct/02/2003312498/-1/ 1/0/RETHINKING%20SOVEREIGNTY.PDF* (last visited October 25, 2023).
6. Allison, Pytlak, Shreya, Lad. 2024. The UN Security Council Discusses Cyber Threats to International Security. *https://www.stimson.org/2024/un-security-council-cyber-threats-to-international-security/* (last visited April 15, 2024).
7. Barlow, John Perry. 1996. A Declaration of the Independence of Cyberspace. *https://www.eff.org/cyberspace-independence* (last visited October 25, 2023).
8. Binxing, Fang. 2018. *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace*. Beijing: Science Press Beijing.
9. Broad, William. 2010. Report Suggests Problems With Iran's Nuclear Effort. NY Times, *https://www.nytimes.com/2010/11/24/world/middleeast/24nuke.html, NYTimes* (last visited 31 August, 2023).
10. *Cyberspace Administration of China*. 2015. The Cyber Perception of President Xi Jinping: To build a cyber power, and let the development benefit the people. *http://www.cac.gov.cn/2015–12/10/c_1117414086.htm* (last visited November 5, 2023).

11. DeWeese, Geoffrey S. "Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence" (2015) 7th International Conference on Cyber Conflict. *https://ccdcoe.org/uploads/2018/10/Art-06-Anticipatory-and-Preemptive-Self-Defense-in-Cyberspace-The-Challenge-of-Imminence.pdf* (last visited October 25, 2023).
12. Digital and Cyberspace Policy Program and Net Politics. The Sinicization of Russia's Cyber Sovereignty Model. *https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model* (last visited October 30, 2023).
13. European Commission. 2022. European Cybersecurity Investment Platform. *https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf* (last visited October 4, 2023).
14. Harrison Dinniss, Heather. 2012. *Cyber Warfare and the Laws of Wars*, New York: Cambridge University Press.
15. Huff, Toby E. 2001. Globalization and the Internet: Comparing the Middle Eastern and Malaysian Experiences. *Middle East Journal* 55: 439–458.
16. Koh, Harold. 2012. Remarks at the U.S. Cyber Command Inter-Agency Legal Conference. *http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/, https://perma.cc/MJS5-XJVA* (last visited October 25, 2023).
17. Kumar, Ankit. 2023. Internet Censorship in China: The Struggle to Swat "Flies" Away. *https://icsin.org/blogs/2023/10/10/internet-censorship-in-china-the-struggle-to-swat-flies-away-2/* (last visited November 5, 2023).
18. Lewis, James Andrew. 2010. Sovereignty and the role of government in cyberspace. *The Brown Journal of World Affairs* 16: 55–65.
19. Ministry of Information and Communications. 2023. The UN discusses cyber attacks on critical infrastructure. *https://mic.gov.vn/pages/tintuc/printpage.aspx?tintucID=158845* (last visited November 5, 2023).
20. Moynihan, Harriet. 2019. The Application of International Law to State Cyberattacks Sovereignty and Non-intervention. Chatham House report. *https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/1-introduction* (last visited October 20, 2023).
21. Nakashima, Ellen. 2013. U.S. and Russia sign pact to create communication link on cyber security. The Washington Post. *https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788–11e2–9df4–895344c13c30_story.html* (last visited October 30, 2023).
22. Nguyen, Tien Duc, Thi Thu Thuy Tran. 2019. Cyber attacks and the principle of prohibition of the use of force in international law. *https://iuscogens-vie.org/2019/04/20/131/#_ftn14* (last visited October 4, 2023).
23. Permanent Delegation of the Socialist Republic of Vietnam in New York – United States. 2019. The UN Security Council discussed the issue of cyberspace stability. *https://vnmission-newyork.mofa.gov.vn/vi-vn/News/*

ConsulateNews/Trang/Hội-đồng-Bảo-an-LHQ-thảo-luận-vấn-đề-ổn-định-không-gian-mạng.aspx?p=38 (last visited November 5, 2023).

24. President of the U.S. 2018. National Cyber Strategy of the U.S of America. *https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf* (last visited October 25, 2023).
25. Roscini, Marco. 2012. *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press.
26. Schmitt, Michael. 2022. The United Kingdom on International Law in Cyberspace *https://www.ejiltalk.org/the-united-kingdom-on-international-law-in-cyberspace/* (last visited October 30, 2023).
27. Schmitt, Michael. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
28. Schneider, Gary P. 2013. *E-Business*. India: Cengage India.
29. Schultz, David, Nataliya Moroz. 2022. Cyberspace and the Future of International Law and Politics. International Policy Digest. *https://intpolicydigest.org/cyberspace-and-the-future-of-international-law-and-politics/* (last visited October 20, 2023).
30. Shen, Yi. 2014. Transform and construction: the design of national cybersecurity strategy and the capacity build in a post-Snowden age. *China Information Security* 5: 41–43.
31. United Nations. General Assembly. 2013. UN GGE Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *https://dig.watch/wp-content/uploads/A_68_98_E.pdf* (last visited October 15, 2023).
32. Vietnam News. 2021. Sovereignty over cyberspace an important part of national sovereignty: official. *https://vietnamnews.vn/society/1095123/sovereignty-over-cyberspace-an-important-part-of-national-sovereignty-official.html*, (last visited November 5, 2023).
33. Xinhua Net. 2014 Address of President Xi Jinping in the Brazil Congress. *http://news.xinhuanet.com/world/2014–07/17/c_1111665403.htm*. (last visited November 5, 2023).