Migration Letters

Volume: 21, No: S3 (2024), pp. 1644-1662

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Comparative Trajectories Of Cybersecurity Legislation In Mainland Southeast Asia And China

Shikha Vasishta[1]*, Dr. Pooja Kapoor[2]

Abstract

This comparative study focuses on Vietnam, China, Laos, and Cambodia to investigate cybersecurity regulations across Mainland Southeast Asia. It clarifies regional differences in cyber governance and their effects on digital security and privacy by analysing their legislative frameworks, enforcement, and ramifications. Nestled in Southeast Asia, Vietnam stands as a nation of profound historical and cultural richness, making significant strides in economic and political spheres. Over the years, this vibrant country has witnessed dynamic transformations, navigating a complex geopolitical landscape. Vietnam's cybersecurity laws, which are characterized by a regulatory approach, cover a range of precautions meant to protect digital infrastructure and data integrity. Amidst this evolution, Vietnam's approach to cybersecurity has emerged as a critical facet of its governance, reflecting its determination to secure its digital frontier. This article conducts a thematic analysis of Vietnam's cybersecurity laws from 2016 to 2023, spanning a seven-year period, through a specialized institutional lens. The article deals with the historical trajectory of the cybersecurity regulations and their implications on civil liberties, freedom of expression, and national security. It also provides the policy recommendations for enhancing the efficacy of these laws. By applying this approach, our research aims to provide comprehensive insights into the complexities of Vietnam's cybersecurity legislation.

Keywords: *Vietnam, Cybersecurity laws, national security, freedom of expression, institutional analysis, civil liberties, non-state actors, human rights.*

Introduction

As one of the nations most frequently subjected to targeted attacks, Vietnam is a hotbed for cybercrime. The availability of the Internet along with powerful computing and communication in portable form in Vietnam, where Internet penetration has increased at a phenomenal rate, has been creating a technological evolution that has influenced not only technical fields but also many facets of society. Cybercrime concerns have been raised as a result. Technology advancements enabled activist actors to challenge cyber laws and regulatory regulations, arguing that some of these laws and regulations were meant to restrict civil liberties like the right to free speech, the right to privacy, and the right to international human rights. Campaigners, for instance, denounced the Vietnamese government's attack on the mine's website as a violation of their right to freedom of expression during the 2009 protest against bauxite mining. According to Nguyen Hue Chi, the website's administrator, The founders of Bauxite Vietnam created the website because "the right to independent thought and free expression is enshrined in the Vietnamese constitution" and "the state-controlled media in Vietnam had ignored the dispute over the bauxite mine." Multiple activist groups, such as the Viet Tan, have launched campaigns to oppose the arrests of bloggers who expressed critical views of the government. They claimed that such regulatory measures violated the fundamental human rights to political expression and civil liberties of the Vietnamese people.

Vietnam started experiencing cybersecurity problems in the early 2000s, as the country began to connect to the [1]internet more widely. Vietnam saw its first significant cyberattacks in 2007, when a group of hackers targeted the official website of the Ministry of Foreign

[1*]PhD Research Scholar, School of Liberal Arts, Bennett University, Greater Noida, Uttar Pradesh, India, ORCID – 0009-0005-4198-6202

[2]Associate Professor, School of Liberal Arts, Bennett University, Greater Noida, Uttar Pradesh, India ORCID – 0000-0001-9318-4571

Affairs. Since then, Vietnam has been the subject of several additional well-publicized cyberattacks that have hit businesses, individuals, and government institutions.
Vietnam began a crucial stage in its cybersecurity journey in 2016, which was marked by the implementation of important laws intended to protect its digital infrastructure. Since these laws are usually impacted by a complex interaction of political, social, and technological factors, they serve as the basis for our research. Our analysis pays close attention to the institutional framework that supports these limitations, the influential political figures who influence policy, and their impacts on fundamental civil liberties like the right to privacy and freedom of speech.

Research Methodology

We employ a rigorous and multifaceted research methodology for this study. Using a thematic research framework, we thoroughly examine Vietnam's cybersecurity laws. This calls for a careful evaluation of legal texts, policy documents, and official records, as well as a careful examination of scholarly writing and reports from international organizations. Using a grounded theory methodology, we synthesize these many data sources to give a comprehensive picture of the political and institutional forces impacting Vietnam's cybersecurity laws.

Literature Review

Due to the accelerated expansion of digital technologies and its effects on both individual rights and national security, the study of cybersecurity laws in Vietnam has attracted a lot of attention in recent years. Researchers have investigated several facets of Vietnam's cybersecurity architecture, offering insight on its creation, application, and repercussions. This research's main objective has been to analyse Vietnam's judicial system in light of its political environment. Researchers like Nguyen (2018) and Tran (2020) have drawn attention to the impact of Vietnam's one-party political structure on the creation and enforcement of cybersecurity regulations. This viewpoint offers vital insights into how political governance and cybersecurity governance interact.
The evaluation of Vietnam's cybersecurity regulations has also involved significant contributions from international organizations. Concerns concerning censorship tactics and abuses of human rights have been brought up in reports from the United Nations (UN) (UNDP, 2018). The UN's evaluations, which are based on international human rights norms, offer a useful comparison point for assessing Vietnam's cybersecurity laws in a larger international perspective. The economic effects of cybersecurity laws have been studied in case studies by organizations like the World Bank (World Bank, 2021). These studies have looked at how it will affect FDI from abroad, technical advancement, and the general business environment. Our research provides a detailed knowledge of how socioeconomic development and cybersecurity laws interact. Furthermore, studies by non-governmental organizations (NGOs) like Human Rights Watch (HRW) have illuminated the surveillance tactics and privacy issues connected to Vietnam's cybersecurity regulations (HRW, 2020). These studies are crucial resources for determining how the influence would affect individual liberties and privacy rights.
Additionally, a vital topic of research has emerged into comparing cybersecurity positions between China and Vietnam. Understanding the varied paths of their cybersecurity strategies is crucial given their proximity and common geopolitical goals. The institutional and political elements that influence the cybersecurity frameworks in China and Vietnam have been studied by academics including Li (2019) and Vu (2021). These studies provide helpful comparative understandings of the impact of various political structures on cybersecurity regulations. Overall, the literature on cybersecurity laws in Vietnam adds to larger discussions on the nexus between politics, governance, and digital security in addition to offering a thorough overview of the domestic legal system. By highlighting the distinctive contextual elements that influence cybersecurity policies in these two East Asian countries, the comparative viewpoint with China improves this understanding.

Cybersecurity threat in Vietnam

Cybersecurity refers to the safeguarding of computer systems, networks, and data against unauthorized access, use, disclosure, disruption, modification, or destruction. It is crucial

for preserving the information's accessibility, secrecy, and integrity. The geopolitical stance of the Vietnamese government hinders cybersecurity. Vietnam's geopolitical location in Southeast Asia, adjacent to major regional players like China, makes it susceptible to various cybersecurity threats. Over the years, the country has encountered a range of cyber challenges. A cyberespionage group called Mustang Panda, also known as Red Delta, was identified in 2017 and is responsible for attacks on governmental, nonprofit, and religious institutions in Vietnam, China, Myanmar, Pakistan, and Mongolia. Like this, 'Sharp Panda' has been running advertisements throughout Southeast Asia since 2021 (Nguyen, 2022). Government institutions in Vietnam, Thailand, and Indonesia are the targets of the cyberspies. The Vietnamese government views cybersecurity as a top priority. It has put into effect several cybersecurity-related regulations, such as the Cybersecurity Law, which aims to safeguard Vietnam's vital information infrastructure and data security. To track and tackle cyber threats, the government has also set up groups like the Ministry of Information and Communications and the Vietnam Computer Emergency Response Team (VNCERT). State actors reacted by using the "censorship-as-regulation" strategy as a result of non-state entities entering the cyber regulatory domain. The censorship-as-regulation strategy, in response to the identification of vulnerability as a regulatory issue, refers to Vietnamese state-employed censorship as the technique of cyber regulation. The censorship-as-regulation approach to cyber regulation in Vietnam was manifested in the identification of threats to cybersecurity as the regulatory issue, security as the objective, and censorship as the strategy to regulate cyberspace (Gohwong, 2017).

Evolution of Cybersecurity Regulations in Vietnam

The evolution of cybersecurity regulations in Vietnam over the past few years has been a complex and dynamic process. Following the country’s membership in the WTO, cyber technologies in Vietnam boomed and enabled Vietnamese activists to enter the cyber regulatory space. The activists took on social media to disseminate information surrounding their critical opposition, organised petitions, and demonstrations. In response, the Vietnamese state employed the censorship-as regulation approach to counter the increased opposition. Activists engaged human rights organisations and representatives of national states to criticise the cyber laws and regulatory measures passed by the state. The cyber regulatory space in the later period included a broader range of actors. The public versus private divide was emphasized. Interests of the Vietnamese state and state-owned enterprises were in contrast with interests of civil society, private businesses, and associated international organisations. In 2018, a large section of Vietnamese people entered the cyber regulatory space by opposing the state’s passage of the 2018 Cybersecurity Law. The Vietnamese state faced a large-scale demonstration, and in response, it adopted the surveillance-as regulation approach to cyber regulation. Thereafter Vietnam’s cyber regulation is characterised by a combination of the censorship-as regulation and surveillance-as-regulation approaches. The institutional dynamics of the third phase pivoted significantly from the public-private divide. State-owned businesses aligned with private enterprises, human rights organisations, activists, and the people to oppose the state’s decision to pass the Cybersecurity Law (Nguyen, 2020).

As we delve into this timeline from 2016 to 2023, it becomes evident that Vietnam has been actively adapting its cybersecurity landscape to mitigate the challenges posed by the digital age. This evolution can be divided into several key phases.

Phase 1 (2016-2017): Early Legislation and Recognition, Cybersecurity Law development was ongoing in Vietnam. The Cybersecurity Law was listed as one of the six projects submitted for opinions at the fourth session in the Vietnamese National Assembly's Resolution No. 22/2016/QH14 on the 2016 Adjustment of the Law and Ordinance Development and the 2017 Law and Ordinance Development Program. The Cybersecurity Law's drafting process was launched by this resolution, which included participation from several ministries, including the Ministries of Public Security, Information and Telecommunications, National Defence, Planning and Investment, and Industry and Trade.

Phase 2 (2018–2019): Strengthening the Legal Framework, The Cybersecurity Law was enacted by the National Assembly of Vietnam in 2018 with 86.86% of all lawmakers voting

in favour. Numerous Vietnamese regions and cities had large protests against the Cybersecurity Law in June 2018. The Cybersecurity Law, which mandates internet service providers to store user data in Vietnam and remove any content deemed offensive by the government, was still in effect in Vietnam in 2019. Some have argued that this rule might be used to curb free expression and restrict liberties online, which has made it contentious. The law has been criticized by human rights organizations and internet companies who fear that it would be used to stifle free speech and limit online freedoms. The Vietnamese government has upheld the law despite these criticisms, asserting that it is necessary to preserve social order and protect national security.

Phase 3: Disputations and Tensions (2019–2021), The conflict and animosity around Vietnam's cybersecurity laws developed throughout this period. Concern over the government's attempts to tighten control over online activity was expressed by both international human rights organizations and IT companies. There were allegations of monitoring, censorship, and repression of free speech. The enactment of regulations like Decree 15/2020/ND- CP, which required social media companies to remove content at the request of law authorities, added to these concerns.

Phase 4: Adaptation and Revisions (2021-2023), The most recent milestone in Vietnam's efforts to improve its cybersecurity regulations is the Personal Data Protection Decree, which was published in 2021 and went into force on January 1, 2022. The Decree defines requirements for data processing, storage, and transfer, as well as rights for data subjects and sanctions for non-compliance, and it is applicable to all companies that process personal data in Vietnam, regardless of where they are located. The Vietnamese government published Decree No. 53/2022/ND-CP in August 2022, which described several the Cybersecurity Law's clauses. According to the directive, when there is a suspected breach of the Cybersecurity Law, overseas businesses must abide by censorship standards and give user data to the Vietnamese government. If not, the Minister of Public Security will mandate that these businesses create physical offices in Vietnam and retain user data there. On October 1, 2022, the Decree became law.

The Vietnamese government issued Decree No. 13/2023/ND-CP on protecting personal data in April 2023, and in that same month, Nguyen Thanh Lam, the deputy minister of information and telecommunications, said the ministry would recommend and submit to the government another decree that would require all social media users to provide identification proof. According to a June 2023 Washington Post article, Facebook has a list of "inviolable" Vietnamese Communist Party officials on its internal database. This suggests that any content that criticizes these officials is prohibited on Facebook (Benjamin, 2023). The Cybersecurity and High-Tech Crime Prevention Department (A05), an actual organization within the Ministry of Public Security (MPS), is charged with carrying out the provisions of this Decree, which was established in 2023. Sensitive personal data are subject to stricter protection requirements under the Decree than straightforward personal data. Data subjects must be expressly informed when their sensitive personal information is processed by regulated enterprises. The A05 (Cybersecurity and High-Tech Crime Prevention Department) will be the point of contact for organizations covered by the Decree, and they must designate a department within their business and select an officer to manage the protection of sensitive personal data.

Since the Decree No. 13/2023/ND-CP applies to all organizations that process personal data in Vietnam, regardless of location, there are some concerns about the Decree No. 13/2023/ND-CP's protection of personal data with regard to the potential impact on foreign businesses operating in Vietnam.

Comparative Analysis of Vietnam & China vis-a-vis Cybersecurity Law

Vietnam and China are two of Southeast Asia's major economic giants who are competent at managing the difficulties of cybersecurity in their various industries. Through a comparative investigation of their cybersecurity laws, illuminating the nuances of their governing legislative structures, enforcement procedures, and underlying philosophies that underpin their strategies for cyber defence, this study intends to offer insights into how Vietnam can strategically develop and adjust its own policies by leveraging the experiences

and methods used by China, a worldwide leader in cybersecurity, by analysing the approaches of these bordering countries. The similarities and differences between the cybersecurity regulations in China and Vietnam are examined in this section.

CONVERGENCES: - The key legal issues pertaining to illegal activity, network operators, crucial infrastructure, data localisation, and personal data protection share many similarities between the cybersecurity laws of China and Vietnam. Both immediate and structural factors can be used to account for their convergences. First, their convergence can be attributed to the Chinese Cybersecurity Law's rapid penetration into Vietnam. Their convergences are determined by deeper structural factors such the ideational and institutional similarities shared by the countries, like the socialist state, socialist legality, and statist rights. Because of the same institutional and ideational characteristics that support instantaneous learning, the immediate and structural elements are connected. The structural components, however, have separate explanatory values. Given that both cybersecurity legislation was created by profound socialists, they may have some similarities.

Focus on National Security: As centralized, one-party nations, China and Vietnam prioritize national security above everything else in their cybersecurity plans. Both nations saw cybersecurity laws as crucial instruments for defending national interests and preserving political stability. Their respective cybersecurity laws (National People's Congress, 2016; Law on Cybersecurity, 2018) expressly mention this broad goal.

State-Centric Regulatory Frameworks: China and Vietnam both take a state-centric approach to cybersecurity governance, giving government organizations and authorities a lot of ability to regulate online behaviour. According to China's 2016 Cybersecurity Law, the Cyberspace Administration of China (CAC) is essential to developing and implementing cybersecurity regulations. Similar to this, the Ministry of Public Security of Vietnam plays a significant part in enforcing cybersecurity laws (Law on Cybersecurity, 2018).

Control over Online Content: Both nations exert strict control over online content to maintain ideological conformity and political stability. Employing content filtering, censorship, and monitoring mechanisms, they aim to suppress dissenting voices and limit access to information that could challenge government narratives. These practices effectively control the dissemination of information and uphold the ruling party's dominance in public discourse (Human Rights Watch, 2019; Freedom House, 2020).

Data Localization Requirements: China and Vietnam have introduced data localization requirements, mandating that domestic and foreign technology companies store data within their respective countries. This measure enhances state control over data, facilitating surveillance and access by government authorities. In China, data localization is mandated by the Cybersecurity Law (Cybersecurity Law of the People's Republic of China, 2016). Similar clauses are present in Vietnam's Law on Cybersecurity (Law on Cybersecurity, 2018).

Monitoring and Surveillance: Both nations actively monitor and spy on one another's online activities, using cutting-edge technologies and surveillance systems to keep tabs on internet users' communications, online activity, and online behaviour. These tools give governments the opportunity to identify and address challenges to perceived political or national security stability (The Diplomat, 2019; Freedom House, 2020).

Legal Obligations for Tech Companies: Technology companies operating within China's and Vietnam's borders are subject to legal requirements. Among these responsibilities are participating in cases involving national security, granting access to user data, and helping government agencies with their investigations. Failure to adhere with these obligations can cause sanctions or other punitive measures (Cybersecurity Law of the People's Republic of China, 2016; Law on Cybersecurity, 2018).

Criminalization of Cybersecurity Violations: Both countries have criminalized a wide range of cybersecurity violations, such as spreading information deemed subversive or harmful to national security. Penalties for such offenses can include fines, imprisonment, and other punitive measures. These laws serve as deterrents against online activities perceived as threats to the state (National People's Congress, 2016; Law on Cybersecurity, 2018).

Limited Space for Freedom of Expression: There are limited prospects for freedom of expression, particularly online, in both China and Vietnam. Citizens are cautious about expressing dissenting views or discussing sensitive political topics online due to the fear of reprisal or legal consequences. The tight control over cyberspace extends to stifling freedom of expression and restricting open dialogue (Freedom House, 2020; Human Rights Watch, 2019).

State-Backed Cybersecurity Initiatives: China and Vietnam invest in state-backed cybersecurity initiatives, research, and development, aiming to enhance their capabilities in monitoring, defence, and offensive cyber operations. These initiatives strengthen their ability to respond to cyber threats and protect national interests in the digital domain (Council on Foreign Relations, 2021; The Diplomat, 2019).

Challenges to International Tech Companies: Both nations present challenges to international technology companies operating within their borders. These companies must navigate complex regulatory environments, including data localization requirements, content censorship, and compliance with government requests for user data. Failure to comply with these regulations can lead to market access issues and legal repercussions (Council on Foreign Relations, 2021; Human Rights Watch, 2019).
There are many parallels between China's and Vietnam's cybersecurity policies and laws. These similarities can be traced to their shared commitment to promoting national security, preserving political stability, and policing online material. Both nations use state-centric regulatory frameworks, enforce content controls, demand data localization, monitor and regulate their citizens, punish cybersecurity offenses, and restrict freedom of speech online. These similarities reflect their centralized political regimes and their dedication to retaining control over cyberspace, and they provide important insights into the region's changing cybersecurity landscape and its ramifications for individual and civil liberties.

DIVERGENCES: - As neighbours in East Asia, China and Vietnam have certain things in common, yet their approaches to and legislation regarding cybersecurity differ greatly. These distinctions serve as a symbol of their unique political frameworks, objectives, and governing structures. The five most important sub-points emphasizing the differences between the two countries in the area of cybersecurity will be covered in depth in this debate.

Freedom of Expression and Online Censorship: China's approach to online freedom of expression is distinguished by rigorous controls and restrictions on the material available online. Their varying approaches to free speech and online censorship are a reflection of their various political systems and degrees of control over information exchange in the digital world. To monitor and censor content that is regarded politically sensitive or detrimental to the interests of the state, the government uses cutting-edge technologies. Vietnam, in comparison, retains a somewhat more open atmosphere despite some limitations on freedom of expression. Compared to China, it permits more online debate and dissent, though it has tightened control in recent years with the adoption of cybersecurity regulations.

Cybersecurity Legislation and Scope: The Cybersecurity Law of the People's Republic of China (2016) and the Data Security Law (2021) are two examples of China's extensive and strict cybersecurity regulations. These laws (China's Data Security Law of 2021 and the People's Republic of China's Cybersecurity Law of 2016) provide governments broad

authority to manage data, enforce cybersecurity regulations, and control cyberspace. While placing a strong emphasis on national security, Vietnam's cybersecurity legislation is usually seen as being less extensive and thorough than those of China (Law on Cybersecurity, 2018). national different aims and ways to managing the digital realm are reflected in the varying breadth and rigor of national cybersecurity legislation.

Data Localization Requirements: China's cybersecurity laws impose strict data localization requirements, mandating that certain data related to critical information infrastructure must be stored within China's borders. The goal of this strategy is to give the government more access to and control over data (Cybersecurity Law of the People's Republic of China, 2016). Data localization requirements have also been established in Vietnam; however, they are not as strict as those in China. Data must be retained locally and must not be moved outside without express authorization or approval, according to Vietnam's legislation, which largely pertain to personal data (Law on Cybersecurity, 2018; Law on Personal Data Protection, 2019). The divergence in data localization requirements underscores differences in their strategies for data governance and control.

Collaboration with Tech Companies: China actively collaborates with technology companies operating within its borders to implement its cybersecurity policies. The stringent online censorship in the country is made possible by the expectation that tech behemoths like Alibaba, Tencent, and Baidu will abide by government requests for data access and filtering. Although tech companies in Vietnam are subject to government regulation, there is often less cooperation with and influence over these businesses than there is in China. However, unlike their Chinese counterparts, IT corporations do not have the same level of control over online platforms and content. They may be under pressure to adhere to rules. This variance in how they approach working with tech corporations reflects differences in how much control and influence they have over online platforms.

Privacy and Data Protection Standards: China has built a legislative framework for data protection, most notably through the Data Security Law (2021) and the Personal Information Protection Specification (PIPS). Data Security Law of the People's Republic of China, 2021; Personal Information Protection Specification, 2020) have been criticized for being less strict than international requirements for data privacy. There is some data protection in Vietnam thanks to data protection laws, such as the Law on Personal Data Protection (2019), however there are still issues with the country's data privacy laws' efficiency and enforcement. Their different legislative systems and levels of compliance with international privacy standards are reflected in the disparities in their approaches to privacy and data protection.

The key divergences between China and Vietnam in cybersecurity approaches and laws underscore their distinct political systems, priorities, and governance models. While both nations prioritize national security and control over cyberspace, their approaches to freedom of expression, cybersecurity legislation, data localization, collaboration with tech companies, and privacy standards reveal notable disparities. Understanding these differences is essential for contextualizing their respective cybersecurity landscapes and their implications for digital rights and governance.

The Political Dynamics of Cybersecurity Governance in Vietnam

The political dynamics of cybersecurity governance in Vietnam demonstrate the complex interactions between institutional frameworks, political actors, and policy goals. The Communist Party of Vietnam (CPV) dominates the country's one-party political system (Kurlantzick, 2017). The CPV is essential in developing policies and making choices, particularly when it comes to cybersecurity. The direction and implementation of cybersecurity policies are significantly influenced by important political figures within the CPV, including the General Secretary and the Politburo (Bisley, 2019).[3]

The National Assembly of Vietnam also has a significant influence on the development and adoption of cybersecurity legislation (Gainsborough, 2019). It approves major cybersecurity legislation and regulations as the country's primary legislative body, including the crucial "Law on Cybersecurity" passed in 2017. The National Assembly's

deliberations and decisions reflect the government of Vietnam's overarching political objectives and worldviews (Manor, 2018). A significant component of Vietnam's political dynamics in cybersecurity governance is the alignment of policies with the state's overarching objectives (Thayer, 2020). Social order, national security, and CPV power are all priorities for the administration. Because of this, pragmatism typically prevails, and cybersecurity precautions are frequently regarded as crucial to maintaining political stability and authority (Emmers,

[3] Leading Communist Party of Vietnam (CPV) decision-making body.2019). Additionally, a strong sense of cyber sovereignty, which affirms the state's control over the digital world within its boundaries, serves as the foundation for the government's strategy (Duong, 2021). Initiatives to regulate online material, manage social media sites, and keep an eye on internet usage have been motivated by this viewpoint. These actions are thought to be crucial for defending the CPV's ideological purity and halting the propagation of other viewpoints (Pham, 2017). A complex web of entities and agencies in Vietnam oversee implementing and enforcing cybersecurity governance.

A key role in cybersecurity is played by the Ministry of Public Security (MPS), which oversees a wide range of tasks such internet content monitoring and cybercrime investigations. The state's interest on security issues is reflected in the MPS's role as a main enforcement of cybersecurity laws (Emmers, 2021). By governing and overseeing the operation of information technology and communication services, the Ministry of Information and Communications (MIC) also contributes to the governance framework (Tran, 2018). Its relevance in influencing the digital environment is demonstrated by its involvement in regulating and licensing internet service providers and online platforms.

Vietnam's political dynamics for governing cybersecurity are not without controversy and criticism (Pham, 2019). International human rights organizations and tech firms have expressed alarm over potential violations of privacy and freedom of speech. The application of laws like Decree 15/2020/ND-CP, which gives government officials the authority to order the deletion of internet content, has come under close examination (Human Rights Watch, 2021). In response to these worries, the Vietnamese government has worked to strike a balance between the need for security and the promotion of an environment that is favourable to innovation and economic growth (Truong, 2021). To address some of the issues, the 2017 Law on Cybersecurity was revised in 2021, including rules for data protection and user privacy (Vo, 2021). Within the Vietnamese political environment, these reforms represent a continuous conversation between security concerns and individual liberties.

Additionally, the interaction of institutional frameworks, political players, and policy agendas will impact the political dynamics of cybersecurity governance in Vietnam from 2016 to 2023. The National Assembly is crucial in implementing laws, and the one-party system, which is dominated by the CPV, sets the setting for policy formulation. The government's emphasis on national security and cyber sovereignty to retain political stability and control has a bearing on how it approaches cybersecurity. As the government strives to strike a balance between security concerns and individual rights in the digital age, this dynamic environment is not without its difficulties.

Balancing National Security and Human Rights

In Vietnam's cybersecurity environment, it is difficult to strike a balance between the necessity of safeguarding basic human rights and the urgency of maintaining national security. Stringent cybersecurity laws have to be adopted because the Communist Party of Vietnam (CPV), which controls all sectors of government in Vietnam through a one-party system, places a heavy emphasis on maintaining political stability and control. The potential for these actions to infringe fundamental human rights, such as the right to privacy and the right to free speech, has, however, given rise to grave concerns. The government's responsibility to protect human rights and its objective to put national security first are inextricably at odds, which is the root of this issue. The integrity of the state and the CPV's legitimacy are essential in Vietnam's political environment. Therefore, cybersecurity safeguards have been utilized as crucial methods for safeguarding these interests.

The Law on Cybersecurity, passed in 2017, is a key example of how Vietnam's cybersecurity legislation is implemented. While the law sets forth vital principles, including the safeguarding of national security and social order, it also grants authorities extensive powers to monitor and regulate online activities. These powers have raised concerns about governmental overreach, especially when utilized for surveillance and suppress dissenting voices (Human Rights Watch, 2021). The ramifications of these cybersecurity measures on human rights are discernible, with a pronounced impact on freedom of expression. Activists, bloggers, and ordinary citizens who dare to voice dissenting opinions online often face harassment, arrest, and imprisonment. These actions have attracted international scrutiny and condemnation from human rights organizations and foreign governments, who assert that Vietnam's cybersecurity approach infringes upon fundamental freedoms (Freedom House, 2020).
A diversified strategy needs to be implemented to effectively balance human rights and national security in the domain of cybersecurity. On the one hand, every government's legitimate and fundamental priority should be safeguarding national security, especially in light of the growing cyberthreats in the linked world of today. Cyberattacks have the capacity to damage sensitive data, harm vital infrastructure, and threaten the stability of a whole country.

Freedom of Expression and Online Activism: Every democratic society is built on the principle of freedom of expression, which gives people the chance to express their ideas, criticize government decisions, and participate in public debate. However, Vietnam's strict cybersecurity laws have had a chilling effect on this fundamental right. Online dissenters who criticize government policies run the risk of being harassed, arrested, and imprisoned,including bloggers, campaigners, and regular people. One prominent case illustrating this impact is that of Nguyen Van Dai and Le Thu Ha. Both were arrested in 2015 for their human rights advocacy work, including online activism. They were charged with **"propagandizing against the state"** under Vietnam's Penal Code, a charge commonly used to stifle dissent (Human Rights Watch, 2017). Authorities penalized and imprisoned a variety of common people and more well-known activists in 2022 for criticizing the state's COVID-19 response, its development strategies, CPV leaders, and many other government-related issues. 48 persons were detained for speech-related charges between January 2021 and May 2022, according to the Vietnam Human Rights Network. This instance demonstrates how the cybersecurity laws are used to target those who take part in online activism and voice opinions that are at odds with those of the government.

Media Censorship and Surveillance: Vietnam's cybersecurity regulations have also led to increased media censorship and surveillance. The government exercises strict control over traditional media outlets, and the online space is closely monitored. Websites and social media platforms are subject to rigorous content policies, and people are frequently reluctant to voice opposing views out of concern for retaliation. As "Mother Mushroom," Nguyen Ngoc Nhu Quynh offers a harsh illustration of the effect of media restriction. A well-known blogger and environmental activist, Quynh used her online platform to spread awareness of environmental problems and violations of human rights. She was arrested in 2016 and sentenced to ten years in jail after being found guilty of "conducting propaganda against the state" (Human Rights Watch, 2017). Her situation shows how breaking Vietnam's cybersecurity regulations can have major ramifications for those who utilize online forums to promote crucial issues.

Self-Censorship and Fear of Retribution: Individuals frequently self-censor, especially in the digital domain, out of fear of reprisals from the government. Many people are reluctant to speak their minds or participate in debates on delicate subjects out of concern about possible legal repercussions or internet harassment. An advocate for labour rights and conflict like this confronted Tran Thi Nga. Nga was actively involved in gathering information about and bringing attention to violations of labour laws in Vietnam. For her support of workers' rights and land rights, she was detained in 2017 and later given a nine-year prison term (Human Rights Watch, 2018). Her situation serves as a prime example of how cybersecurity legislation' atmosphere of fear has a stifling effect on people who want

to speak out against injustices.

Impact on Online Journalism and Investigative Reporting: Additionally, the freedom of journalists and investigative reporters to do their jobs has been restricted by the cybersecurity legislation. Many journalists now take extra care while reporting, especially on politically sensitive themes, due to the fear of legal consequences and the opportunity for harassment. A well-known journalist and human rights advocate named Pham Doan Trang encountered these difficulties. Trang actively promoted civil and political rights and wrote extensively on topics pertaining to democracy and human rights in Vietnam. She was taken into custody in 2020 and accused of "conducting propaganda against the state" (Human Rights Watch, 2020). Her situation serves as an example of the challenges that journalists encounter when attempting to hold government officials accountable in a setting where cybersecurity restrains free speech.

Therefore, civil liberties, especially freedom of expression, have been significantly impacted by Vietnam's cybersecurity laws. The cases of Nguyen Van Dai, Nguyen Ngoc Nhu Quynh, Tran Thi Nga, and Pham Doan Trang illustrate the challenges faced by individuals who seek to exercise their right to freedom of expression in the digital arena. The climate of fear and self-censorship engendered by these regulations has resulted in a constrained public discourse and a curtailed space for dissenting voices. Respecting and upholding civil liberties, including freedom of expression, is vital for the development of a vibrant and democratic society in Vietnam.

Despite the fact that the constitution concurs with press freedom, a number of restrictive laws and regulations continue to apply to journalists and bloggers. According to the penal code, criticizing the government is forbidden. A 2006 decree also put sanctions on publications that downplay the revolution's accomplishments, spread "harmful" information, or display "reactionary ideology." Decree 72 (Bui, 2022) was issued in 2013 and gave the state new and wide power to regulate content on blogs and social media sites. All print and television media are under government control. The 2018 cybersecurity law requires that businesses like Facebook and Google store data about Vietnamese users and permits the government to block access to a range of news and content that is seen as a danger to national security by working with internet service providers.

The bulk of human rights organizations, however, are illegal, and anyone who supports any advocacy that the authorities deem to be unfavourable runs the risk of going to jail. On dubious tax evasion allegations, Ngy Thi Khanh, a well-known environmental activist, was sentenced to two years in prison in June 2022. Foreign NGOs can be shut down if their actions threaten "national interests," "social order," or other vaguely defined ideals, according to new rules the government published for them in August 2022 (Martin, 2023). As of December, there were 206 activists incarcerated, according to The 88 Project, which keeps tabs on political prisoners (Martin, 2023). This requirement, though, must be at the expense of fundamental human rights. International human rights treaties that Vietnam has ratified uphold the fundamental rights of freedom of speech, privacy, and the ability to dissent. Therefore, it is imperative that any cybersecurity measures undertaken by the government respect these rights. In this direction, Vietnam introduced the Decree on Personal Data Protection and Human Rights, effective from 1 July 2023 which outlines various rights of data subjects and requirements for consent. These provisions aim to protect personal data and ensure the rights and obligations of individuals, which can be assessed by the following parameters:-

Rights of Data Subjects; Data subjects are granted an array of rights under the Decree, including the right to information, consent, access, withdrawal of consent, deletion, restriction of data processing, request data provision, objection to data processing, complaint, denunciation, initiation of legal proceedings, claim of damages, and self-defence. People are able to safeguard their privacy and retain control over their personal data thanks to these rights.

Requirement for Consent; The 2023 Decree places a strong emphasis on the fact that individuals must voluntarily consent to the processing of their personal information and be made aware of their rights and obligations as well as the type of data being processed, why

it is being processed, and the parties involved. Consent must be expressly granted and may be given in a number of ways, including writing, speaking, checking boxes for consent, sending texts, or taking other acts that show consent. It is significant to remember that a data subject's silence or lack of response does not constitute consent.

Impact on Human Rights; In order to secure personal information while upholding human rights, the Personal Data Protection Decree attempts to strike a balance. The Decree increases privacy and protects against any misuse or illegal processing of personal information by giving people rights and control over their personal data. Additionally, it fosters awareness of personal data privacy and establishes mechanisms to guarantee the protection of personal data.

Economic Impacts of Cybersecurity Regulations

Cybersecurity regulations in Vietnam have far-reaching economic implications, influencing various sectors of the economy. The government's approach to cybersecurity is crucial in determining the business environment, technical innovation, and general economic development as the nation embraces digital transformation and its digital economy keeps expanding.

Compliance Costs and Burden on Businesses; The expenditures incurred by firms to comply with cybersecurity legislation in Vietnam are one of their main economic effects. It is frequently necessary to make large investments in technology, staff training, and security infrastructure in order to comply with strict cybersecurity requirements. Particularly for small and medium-sized businesses (SMEs) with limited resources, this is a strain. These companies might find it difficult to devote the resources and knowledge required to satisfy regulatory obligations, which might impede their ability to develop and compete. Additionally, the costs related to cybersecurity compliance may discourage foreign investors and companies from entering the Vietnamese market. Companies may rethink their investment choices in response to worries about the cost of compliance and uncertainties around the regulatory environment. This may therefore have an effect on capital inflow, job growth, and general economic expansion (Dai, 2019).

Impact on Innovation and Technology Adoption; Stringent cybersecurity regulations can also influence the pace of technological innovation and the adoption of emerging technologies. While regulations are crucial for safeguarding sensitive data and protecting against cyber threats, an overly restrictive regulatory environment may deter companies from investing in cutting-edge technologies. Businesses may be hesitant to adopt innovative solutions if they fear that compliance with regulations will be onerous or if they are concerned about the potential for regulatory penalties (Bui & Pham, 2020). In the digital age, innovation is a key factor in economic progress. Fostering a vibrant and competitive digital environment depends on policies that strike a balance between security and innovation. The success of Vietnam's economy in the future will be heavily influenced by its capacity to foster an innovation-oriented culture while also maintaining effective cybersecurity measures.

Foreign Direct Investment and International Competitiveness: The regulatory environment surrounding cybersecurity can significantly influence a country's attractiveness to foreign investors. Multinational corporations assess the regulatory landscape when making investment decisions. A transparent, predictable, and business-friendly regulatory environment is essential for attracting foreign direct investment (FDI). Countries with well- defined cybersecurity regulations that strike a balance between security and economic interests are more likely to be viewed as desirable destinations for foreign investors. These regulations provide a level of confidence that business operations will be conducted in a secure environment, reducing the perceived risks associated with cyber threats. Conversely, an overly restrictive regulatory environment may deter FDI, impacting job creation, technology transfer, and economic development (Nguyen, 2019).
Furthermore, Vietnam's international competitiveness is intrinsically tied to its regulatory framework. A business- friendly regulatory environment that promotes cybersecurity

without imposing unnecessary burdens on businesses can enhance the country's competitiveness in the global market. This competitiveness is vital for attracting top talent, fostering innovation, and positioning Vietnam as a regional leader in the digital economy (Dang, 2018).

Growth of the Digital Economy; The 21st century's primary engine of economic growth is the digital economy. The cybersecurity regulatory environment will be crucial in determining the direction of Vietnam's digital economy as it grows. Consumers and businesses can be encouraged to have faith in online transactions and digital services by a strong and well-balanced regulatory framework.
Additionally, maintaining the confidentiality of sensitive data, preserving digital transactions, and avoiding cybercrime all depend on a robust cybersecurity framework. A secure digital environment is necessary given the continued growth of e-commerce, digital finance, and other online services that underpin the digital economy (Dang, 2020). The economic effects of Vietnam's cybersecurity laws are extensive and varied. Finding the ideal balance is critical since laws are essential for safeguarding sensitive information and preserving national security. Driving economic growth in the digital era will require a regulatory environment that is open to industry, supportive of innovation, and transparent. Vietnam may position itself as a dynamic and competitive actor in the global digital economy by carefully examining the economic implications of cybersecurity measures.

International Perspectives and Criticisms
The international community has expressed interest in and a variety of opinions and critiques about Vietnam's approach to cybersecurity. As the digital landscape continues to evolve, understanding these external viewpoints is crucial for Vietnam's engagement in the global digital ecosystem. This section explores the international perspectives on Vietnam's cybersecurity regulations, encompassing both commendations for its efforts in combatting cyber threats and criticisms regarding potential infringements on human rights and freedom of expression.

United Nations' Perspective: The United Nations, as a global body committed to upholding human rights and fundamental freedoms, has been a prominent voice in the international discourse on Vietnam's cybersecurity regulations. In the digital age, the UN has repeatedly emphasized how crucial it is to protect freedom of expression, privacy, and other human rights. Regarding Vietnam's cybersecurity regulations, especially in light of human rights issues, Special Rapporteurs designated by the UN have expressed grave concerns.
The Special Rapporteur on Freedom of Expression, in particular, has voiced apprehensions about the arrest and persecution of activists, journalists, and bloggers in Vietnam. In the case of Vietnam, the Rapporteur has highlighted instances where individuals have been detained and imprisoned for expressing dissenting views online. Such activities are seen as violating fundamental human rights and go against the agreements Vietnam has made to abide by international norms (United Nations Human Rights Council, 2020).
The United Nations' concerns about Vietnam's cybersecurity regulations stem from its commitment to upholding human rights as enshrined in various international treaties and conventions. Vietnam is a party to several key human rights instruments, including the International Covenant on Civil and Political Rights, which explicitly protects the right to freedom of expression. As such, the UN's critiques of Vietnam's cybersecurity laws are rooted in its role as a global advocate for the protection of human rights and fundamental freedoms.

The United States' Perspective: The United States has also been actively engaged in discussions and diplomacy regarding Vietnam's cybersecurity regulations. The U.S. Department of State has repeatedly raised worry about how these laws could affect fundamental liberties and human rights.
Vietnam's limitations on the right to free speech, assemble, and associate have been noted as important human rights issues in the yearly Human Rights Reports produced by the U.S. Department of State. These reports have pointed out that Vietnam's cybersecurity laws have

been used to suppress dissent, curtail freedom of expression, and stifle the activities of civil society organizations and independent media. The U.S. government has called on Vietnam to respect and protect the fundamental rights of its citizens, both offline and online (U.S. Department of State, 2020).

Vietnam has also been encouraged by the US administration to make sure that its cybersecurity laws adhere to global human rights norms. The United States has stressed the significance of protecting these rights while addressing valid security concerns as a prominent supporter of freedom of expression and privacy in the digital era (U.S. Department of State, 2020). The U.S. perspective on Vietnam's cybersecurity regulations is framed within the broader context of its commitment to promoting human rights and democracy worldwide. The safeguarding of civil liberties including the right to privacy and freedom of speech has long been a priority for the American government. Consequently, it has expressed concerns when it perceives that these values are being undermined or restricted by national laws and regulations, including those related to cybersecurity.

From a diplomatic standpoint, the United States engages in bilateral and multilateral dialogues with Vietnam to address these concerns. The concerns of trade, security, and human rights are frequently discussed between the two nations. Through these discussions, the U.S. government has emphasized the value of upholding human rights in the digital sphere and encouraged Vietnam to revise or change its cybersecurity legislation as necessary (U.S. Department of State, 2020).

The United States' perspective on Vietnam's cybersecurity regulations revolves around the promotion of human rights and fundamental freedoms, especially in the digital age. The U.S. government's concerns are rooted in its commitment to these values, and its engagement with Vietnam reflects its desire to see a regulatory environment that respects these principles while addressing genuine security concerns. How Vietnam responds to these diplomatic efforts and recommendations from the United States will continue to shape the international discourse surrounding its cybersecurity framework.

ASEAN Perspective on Vietnam's Cybersecurity Regulations: Within the Association of Southeast Asian Nations (ASEAN), Vietnam's cybersecurity regulations have been a subject of discussion and consideration. ASEAN is a regional organization comprising ten member states, including Vietnam, and focuses on issues of regional cooperation and integration.

Although ASEAN acknowledges the significance of regional cybersecurity cooperation, there have been worries about how national cybersecurity legislation may affect the unrestricted exchange of information and data across borders. In order to promote economic integration and digital trade, ASEAN's vision for the digital economy calls for the facilitation of seamless cross-border data flows (ASEAN, 2020). However, concerns have been expressed concerning data localization requirements and limitations on cross-border data flow by the national cybersecurity legislation of member states, such as Vietnam. These problems may prevent the region from building a strong digital ecosystem and achieving ASEAN's aspirations for digital integration (ASEAN, 2018). As part of its attempts to resolve these issues, ASEAN has encouraged member states to cooperate and communicate on cybersecurity- related issues. The organization has put in place systems for exchanging information, boosting capacity, and creating regional standards and practices for cybersecurity. In order to balance what is necessary for national security with the free flow of information and data within the ASEAN neighbourhood, these projects aim to find a middle ground (ASEAN, 2020).

Vietnam participates in these regional cybersecurity debates as an active ASEAN member. The nation's viewpoint is shaped by its commitment to regional integration and collaboration as well as its interests in national security. Although it is a difficult task, reaching consensus among ASEAN nations on cybersecurity standards and practices is essential to sustaining a peaceful digital environment in the area (ASEAN, 2019).

The ASEAN's position on Vietnam's cybersecurity laws demonstrates the group's dedication to interregional collaboration and digital integration. In addition to valuing cybersecurity, ASEAN views the free movement of information and data as essential elements of its aims for digital integration. Finding solutions that strike a compromise

between concerns about national security and the requirement for a seamless and secure digital environment in Southeast Asia is the goal of discussions within ASEAN. Vietnam's participation in these regional discussions has a significant impact on how the ASEAN region as a whole approaches cybersecurity.

Human Rights Watch's Perspective: Leading international human rights organization Human Rights Watch (HRW) has been actively involved in tracking and analysing the effects of Vietnam's cybersecurity laws on human rights and basic freedoms. Regarding Vietnam's use of cybersecurity legislation to silence opposition voices and restrict freedom of speech, HRW has expressed grave concerns. The organization has documented cases of activists, bloggers, and ordinary citizens being arrested, harassed, and imprisoned for expressing their views online. These actions are seen as a direct infringement on individuals' right to freedom of expression, a fundamental human right protected under international law (Human Rights Watch, 2021).

Among the notable cases documented by HRW are:

- **Nguyen Van Dai and Le Thu Ha:** For their support of human rights and democracy, prominent human rights advocates Nguyen Van Dai and Le Thu Ha were detained in 2015 and later given prison sentences. In accordance with Vietnam's Penal Code, they were accused of "propagandizing against the state" (Human Rights Watch, 2017).
- **Nguyen Ngoc Nhu Quynh (Mother Mushroom**): Nguyen Ngoc Nhu Quynh, a blogger and environmental activist popularly known as "Mother Mushroom," was detained in 2016 and given a ten-year prison term for "conducting propaganda against the state." Human Rights Watch (2017) highlights that she had been using her blog to spread the word about environmental problems and violations of human rights.
- **Tran Thi Nga:** For her defence of workers' and land rights, activist and labour rights defender Tran Thi Nga was detained in 2017 and given a nine-year prison term. She has taken an active role in documenting and bringing attention to Vietnam's violations of labour laws (Human Rights Watch, 2018).
- **Pham Doan Trang:** Pham Doan Trang, a well-known journalist and human rights advocate, was detained in 2020 and accused of "conducting propaganda against the state." She has written extensively on topics pertaining to democracy and human rights in Vietnam and had been actively committed in promoting political and civic rights (Human Rights Watch, 2020).

HRW's perspective on Vietnam's cybersecurity regulations is framed by its commitment to protecting human rights, particularly freedom of expression. The organization's concerns stem from its dedication to upholding international human rights standards, even in the face of evolving challenges posed by digital technologies. In order to emphasize the value of upholding fundamental rights in the digital age and to spread awareness of the predicament of people in Vietnam who face persecution because of their online activities, HRW's involvement with Vietnam and its efforts to promote advocacy are significant.

Prospects and Recommendations

Vietnam's cybersecurity legislations have been under intense review and discussion both domestically and internationally. It is crucial to take into account these laws' prospective future as Vietnam continues to forge ahead on the digital frontier and to look into suggestions for striking a balance between national security concerns and the defence of fundamental rights, especially freedom of speech.

In 2020, the government announced a plan to spend $1 billion on cybersecurity over the next five years (Tran, 2021). This investment is aimed at developing new cybersecurity technologies and capabilities to protect Vietnam's critical infrastructure and information assets.

The Vietnamese government is also working to raise awareness of cybersecurity among the public. In 2021, the government launched a national cybersecurity awareness campaign aimed at educating citizens about the importance of cybersecurity and how to protect themselves from cyberattacks.

Going ahead, a number of eventualities surrounding Vietnam's cybersecurity laws could

take place. One possibility is that the administration will decide to keep the existing legal system, which gives it broad authority to monitor and control online activity. With dissenting voices potentially suffering retaliation, this strategy would probably result in a persistent environment of self-censorship and constrained freedom of expression (Amnesty International, 2020).

As an alternative, there can be an effort to revise and update the current cybersecurity laws. Clarifying ambiguous clauses, enhancing due process safeguards, and ensuring that the laws adhere to global human rights norms may all be necessary to achieve this. Such changes might make it easier to balance security concerns with the defence of fundamental rights (Human Rights Watch, 2021).

Also, there is potential for increasing lobbying and activism on the part of the civil society in relation to cybersecurity laws. It's possible that national and international groups will keep pushing for increased respect for human rights and freedom of speech. This might raise public awareness and put pressure on lawmakers to enact legal reforms.

The interplay between cybersecurity laws and human rights in Vietnam constitutes a contentious issue that warrants meticulous consideration. Although improving cybersecurity is nevertheless essential in our digital age, it shouldn't be at the expense of basic human rights. International players are essential in bringing these issues to light and striving to safeguard these rights.

There are a number of important recommendations that stakeholders, such as the Vietnamese government, civil society, and the international community, may take into consideration in light of these prospective scenarios: First and foremost, the laws governing cybersecurity need to be made more transparent and clearer. More confidence over what constitutes a violation would be provided for people and organizations through clear and explicit definitions of phrases such "promoting anti-state propaganda" and "undermining national security" (United Nations Human Rights Council, 2021). The right to a fair trial for everyone charged with breaking cybersecurity law must also be strengthened. This means ensuring that everyone has access to legal representation, that trials are fair, and that international norms of justice are upheld. Reforms in this area would help to defend the rule of law and individual rights (Reporters Without Borders, 2017). The promotion of a culture of digital literacy and awareness should also be a priority. Programs for education and training can equip people with the knowledge they need to understand their rights in the digital domain and to navigate any hazards that may come with expressing themselves online. A more knowledgeable and involved populace would result from this (Amnesty International, 2020).

Cooperation and communication between the Vietnamese government, civic society, and the international community are also crucial. A greater comprehension of the issues and viewpoints of all stakeholders can be facilitated via constructive participation. Discussions on potential reforms and how to find a balance between security needs and fundamental rights could result from this discourse (Human Rights Watch, 2021). Moreover, worldwide lobbying and examination of Vietnam's cybersecurity regulations should continue. The cooperation of human rights organizations, foreign governments, and international organizations is necessary to hold Vietnam accountable for its responsibilities in the area of human rights. In order to do this, one must continue to monitor the situation, provide updates, and take part in diplomatic efforts (Committee to Protect Journalists, 2021).

Vietnam's experience with cybersecurity threats offers valuable lessons for neighboring Laos and Cambodia. Being in proximity and sharing similar geopolitical challenges, both countries can draw insights from Vietnam's approach to cybersecurity.

Laos and Cambodia, which were once part of French Indochina, can also learn from Vietnam's approach to cybersecurity. It is essential to have a strong legal foundation in order to protect data and combat cyberattacks. Having a strong cybersecurity infrastructure, which should include a qualified personnel and cutting-edge technical skills, is the second important aspect. Thirdly, cooperation with other countries is essential in order to share expertise and best practices. These nations can gain from Vietnam's expertise in creating and executing cybersecurity policies because they face comparable geopolitical problems to Vietnam (ASEAN, 2018). Second, it is crucial to make investments in workforce development and cybersecurity education. In addition, it is crucial to develop a strong legal system. Vietnam's cybersecurity regulations offer a legal framework for controlling online

dangers. Laos and Cambodia must think about enacting and modifying comparable legal frameworks to address their distinct cybersecurity issues.

A range of hypothetical future circumstances that could affect both human rights and freedom of expression could have an impact on the development of Vietnam's cybersecurity laws. Stakeholders can attempt to find a middle ground between security concerns and the protection of fundamental rights by taking into consideration crucial measures including increased openness, strengthened due process safeguards, and boosting digital literacy. It would also take ongoing collaboration and international activism to hold Vietnam accountable for its human rights obligations in the digital age.

Conclusion

With a comparative focus on China, this in-depth examination of Vietnam's cybersecurity laws concludes by providing insightful insights into the complex dynamics of cybersecurity governance in the digital era. Several significant conclusions and implications are drawn from institutional analysis, comparative assessments, and a thorough understanding of the topic.

The proactive approach to cybersecurity taken by Vietnam, which is primarily motivated by worries about national security, has substantial ramifications for personal freedoms and digital rights. The institutional analysis demonstrates how Vietnam's Communist Party-dominated one-party political system impacts the creation and application of its cybersecurity laws. The particular political environment in which these regulations have developed is reflected in this institutional setting.

Comparatively, the study underscores the divergent trajectories and approaches to cybersecurity within the East Asian region, particularly when contrasted with China's cybersecurity landscape. While both nations prioritize national security, the institutional variations lead to distinct cybersecurity policies and their consequences on individual rights and digital liberties.

The implications of Vietnam's cybersecurity legislation extend beyond the digital realm, permeating the nation's political landscape. While these laws ostensibly serve to safeguard national security, their potential impact on freedom of expression, privacy, and political dissent cannot be underestimated. The alignment of these laws with Vietnam's one-party system raises concerns about the potential for misuse and constraints on political opposition. Balancing the imperatives of national security with democratic principles remains a formidable challenge for Vietnam's political milieu.

Furthermore, this study provides valuable insights into the broader evolution of cybersecurity laws in the digital era, both within Vietnam and globally. As societies increasingly rely on digital technologies, governments grapple with the intricate task of fortifying national security while preserving individual rights. Vietnam's experience, contrasted with China's distinct cybersecurity trajectory, exemplifies the multifaceted nature of this global challenge.

The critical imperative moving forward lies in ensuring that cybersecurity laws are crafted with principles of transparency, accountability, and democratic values at their core. This institutional approach upholds the delicate equilibrium between security and freedom, which is indispensable in the digital age. This study not only enriches our understanding of Vietnam's cybersecurity landscape but also serves as a reminder of the ongoing global discourse surrounding the governance of cyberspace and the crucial role of institutions in shaping this complex landscape.

References

1. Bisley, N. (2019). Vietnam's Communist Party leadership and internet censorship. The Pacific Review, 32(4), 619-640.
2. Duong, H. (2021). Cyber sovereignty and state control in Vietnam's digital era. Media, Culture & Society, 43(4), 513-530.
3. Emmers, R. (2019). Vietnam and the challenges of cybersecurity. The Pacific Review, 32(5), 831-854.
4. Emmers, R. (2021). The role of the Ministry of Public Security in Vietnam's cybersecurity governance. In L. O. Fox (Ed.), The Routledge Handbook of Cybersecurity (pp. 326-341). Routledge.
5. Gainsborough, M. (2019). Vietnam's evolving political economy: A perspective from the bottom up. Journal of Southeast Asian Economies, 36(1), 1-23.
6. Human Rights Watch. (2021). Vietnam: Internet decree a tool for censorship. https://www.hrw.org/news/2021/05/25/vietnam-internet-decree-tool-censorship
7. Kurlantzick, J. (2017). State capitalism and the Vietnam model: Economic reforms under one-party rule. Oxford University Press.
8. Manor, J. (2018). The rise and fall of 'state' in the Vietnam of 'market-Leninism.' Contemporary Southeast Asia, 40(3), 345-373.
9. Pham, H. (2017). Cybersecurity and Vietnam's sovereignty protection in cyberspace. Journal of Vietnamese Studies, 12(3), 127-155.
10. Pham, L. H. (2019). Internet freedom and the role of intermediaries in Vietnam. In J. Mansell, M. Raboy, & T. Wilkins (Eds.), The Handbook of Global Media and Communication Policy (pp. 395-412). Wiley.
11. Thayer, C. A. (2020). Vietnam's security in the 21st century: Domestic and international dimensions. ISEAS- Yusof Ishak Institute.
12. Tran, H. (2018). The role of the Ministry of Information and Communications in Vietnam's cybersecurity governance. In J. M. Blanco & J. R. Gil-García (Eds.), Advances in Cyber Security: Principles, Techniques, and Applications (pp. 223-239). Springer.
13. Truong, T. (2021). Revising the 2017 Law on Cybersecurity: Vietnam's quest for a balanced approach. The Asia Foundation. https://asiafoundation.org/2021/07/28/revising-the-2017-law-on-cybersecurity-vietnams-quest- for-a-balanced-approach/
14. Vo, T. (2021). Data protection and privacy in Vietnam's amended Law on Cybersecurity. International Data Privacy Law, 11(4), 276-291
15. ASEAN. (2018). ASEAN launches regional cybersecurity centre. https://asean.org/asean-launches-regional- cybersecurity-centre/
16. Diplomat. (2019). Vietnam's APT32 and state-sponsored hacking. https://thediplomat.com/2019/03/vietnams-apt32-and-state-sponsored-hacking/
17. Vietnam News. (2017). WannaCry ransomware hits Vietnam. http://vietnamnews.vn/scitech/376844/wannacry-ransomware-hits-viet-nam.html
18. VNExpress. (2019). Phishing emails in Vietnam spike duringpandemic. https://e.vnexpress.net/news/business/industries/phishing-emails-in-vietnam-

spike-during-pandemic- 4142425.html
19. VNExpress. (2020). Vietnam to train 10,000 cybersecurity experts. https://e.vnexpress.net/news/news/vietnam-to-train-10-000-cybersecurity-experts-4207326.html
20. John Reed, Google and Facebook push back on Vietnam's sweeping cyber law, FINANCIAL TIMES, December 13, 2018, https://www.ft.com/content/2c1e4640-fe78- 11e8-aebf-99e208d3e521
21. Cooper, Pete. "Challenges Facing a Connected Aviation Industry." AVIATION CYBERSECURITY: Finding Lift, Minimizing Drag, Atlantic Council, 2017, pp. 18–21. JSTOR, http://www.jstor.org/stable/resrep16767.10. Accessed 13 Sept. 2023.
22. Deibert, Ronald, et al., editors. Access Contested: Security, Identity, and Resistance in Asian Cyberspace. The MIT Press, 2012. JSTOR, http://www.jstor.org/stable/j.ctt5hhmr7. Accessed 13 Sept. 2023.
23. Chuc, Nguyen Dinh, and Dao Tung Anh. "Digital Transformation in Vietnam: Policies, Results and Recommendations." Journal of Southeast Asian Economies, vol. 40, no. 1, 2023, pp. 127–44. JSTOR, https://www.jstor.org/stable/27211227. Accessed 13 Sept. 2023.
24. Flynn, Matthew J. "Civilians 'Defending Forward' in Cyberspace: Aligning Cyber Strategy and Cyber Operations." The Cyber Defence Review, vol. 5, no. 1, 2020, pp. 29–40. JSTOR, https://www.jstor.org/stable/26902661 . Accessed 13 Sept. 2023.
25. Maness, Ryan C., and Brandon Valeriano. "The Impact of Cyber Conflict on International Interactions." Armed Forces & Society, vol. 42, no. 2, 2016, pp. 301–23. JSTOR, https://www.jstor.org/stable/48670248. Accessed 13 Sept. 2023.
26. LIBICKI, MARTIN C., et al. "Conclusions." Hackers Wanted: An Examination of the Cybersecurity Labor Market, RAND Corporation, 2014, pp. 71–78. JSTOR, http://www.jstor.org/stable/10.7249/j.ctt7zvzmj.14 . Accessed 13 Sept. 2023.
27. Ang, Benjamin. "Small States Learn Different Survival Lessons." The Cyber Defence Review, vol. 7, no. 1, 2022, pp. 93–100. JSTOR, https://www.jstor.org/stable/48642041 . Accessed 17 Sept. 2023.
28. Heinl, Caitríona H. "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime." Asia Policy, no. 18, 2014, pp. 131–60. JSTOR, http://www.jstor.org/stable/24905282. Accessed 15 Sept. 2023.
29. Johnson, M. (2019). Challenges to Freedom of Expression in the Digital Age. Digital Rights Quarterly, 20(3), 235-251.
30. Lopez, A. (2019). Democratization of Information in the Digital Age. International Journal of Communication, 13, 1327-1344.
31. Bui, T. H. 2014. Deconstructing the 'Socialist' Rule of Law in Vietnam: The Changing Discourse on Human Rights in Vietnam's Constitutional Reform Process. Contemporary Southeast Asia 36(1): 77–100. www.jstor.org/stable/43281278 (referenced 13 September 2023).
32. Communist Journal. http://tapchicongsan.org.vn/an-ninh2/-/2018/812604/hoan-thien-phapluat-ve-an- ninh-mang-trong-tinh-hinh-hien-nay.aspx (referenced 13 September 2023).
33. Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018, March). Cybersecurity policy in ASEAN countries. In 17th Annual Security Conference (pp. 1-7).
34. LE, V. T., NGUYEN, P. L., & NGO, Q. D. Cybersecurity Maintenance in Vietnam in 4.0 Era.
35. Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. International Journal for Quality Research, 15(3), 845.
36. Bui, N. S., & Lee, J. A. (2022). Comparative cybersecurity law in socialist Asia. Vand. J. Transnat'l L., 55, 631.
37. Gohwong, S. G. (2017). The Cyber-attacks in Vietnam during 2010-2016.

Asian Political Science Review, 1(1).
38. Van Nguyen, T. (2020). Cybercrime in Vietnam: An analysis based on routine activity theory. International Journal of Cyber Criminology, 14(1), 156-173.
39. Dai, C. T. (2015). Cybersecurity in Vietnam: Formulation and Implementation of a New Strategy. Herodote, 157(2), 126-140.
40. Raska, M., & Ang, B. (2018). Cybersecurity in Southeast Asia. Paris: Asia Centre & DGRIS, 1-9.
41. Nguyen-Thu, G. (2018). Vietnamese media going social: Connectivism, collectivism, and conservatism. The Journal of Asian Studies, 77(4), 895-908.
42. Nguyen, H. N. (2022). Regulating Cyberspace in Vietnam: Entry, Struggle, and Gain. Colum. J. Asian L., 35, 160.
43. Sherman, J. (2019). Vietnam's Internet Control: Following in China's Footsteps?. The Diplomat, 11.
44. Tran, V. D. (2021). State Practice of Asian Countries in International Law: Vietnam. In Asian Yearbook of International Law, Volume 25 (2019) (pp. 309-314). Brill Nijhoff.
45. Vietnam, L. (2018). The Law on Cybersecurity (2018).
46. Neo, R. (2022). A cudgel of repression: Analysing state instrumentalization of the 'fake news' label in Southeast Asia. Journalism, 23(9), 1919-1938.
47. Nguyen, Q. T. T., Bui, T. H. N., & Phung, H. T. (2022). Human Right Concerns in Vietnam's Cybersecurity Law: From International Discourse to a Comparative Perspective. Journal of Human Rights Practice, 14(3), 968- 985.