DOCTORAL THESIS

Legitimizing the Vietnam's Cybersecurity Law: Media Narratives and System Justification

NGUYEN, Quang Minh Nguyet

Date of Award:
2025

Legitimizing the Vietnam's Cybersecurity Law:

Media Narratives and System Justification

NGUYEN Quang Minh Nguyet, Moon

A thesis submitted in partial fulfilment of the requirements

for the degree of

Doctoral of Philosophy

Principal Supervisor:

Prof. Guo Steve Z S (Hong Kong Baptist University)

November 2024

DECLARATION

I hereby declare that this thesis represents my own work which has been done after registration for the degree of PhD at Hong Kong Baptist University, and has not been previously included in a thesis or dissertation submitted to this or any other institution for a degree, diploma or other qualifications.

I have read the University's current research ethics guidelens, and accept responsibility for the conduct of the procedure in accordance with the University's Research Ethics Committee (REC). I have attempted to identify all the risks related to this research that may arise in conducting this research, obtained the relevant ethical and/or safety approval (where applicable), and acknowledge my obligations and the rights of the participants.

Signature

November 2024

ABSTRACT

This thesis investigates the justification strategies employed by the Vietnamese party-state to legitimize the Vietnam Cybersecurity Law (VCSL) promulgated in 2018. Grounded in System Justification Theory (SJT), this study explores how state-sponsored media constructs narratives to resonate with people's cognitive and psychological factors that drive them to rationalize, bolster, and defend existing social and political arrangements, even at the expense of fundamental human rights and individual's wellbeing.

The thesis consists of three interconnected studies. Aims to provide a comprehensive picture of the VCSL and contextual factors around law enforcement, the Study 1 undertakes a comparative approach to compare state-sponsored and international media discourses. The findings underline a stark contrast between the hypersecuritization narratives emphasized by threat politics in Vietnamese state-sponsored media and the human rights and economic concerns highlighted by international media. The Study 2 investigates the positioning of laypeople, portraying them as powerless and vulnerable to cyber threats in contrast to the powerful leadership of the party-state, thereby justifying the existential need for a protective and authoritative state. It also examines the construction of political allegiance and the alienation of hostile forces, further reinforcing the legitimacy of the VCSL. The Study 3 identifies key justification strategies, including rationalization, moralization, authorization, denial of system shortcomings, and stereotyping/delegitimization, and analyses their interconnectedness in supporting system justification.

To achieve research objectives, the thesis employs a mixed-method approach integrated content analysis, corpus-based critical discourse analysis, and critical discourse analysis in the three studies. The findings reinforce a mechanism of system justification, by which, the party-state exploits existential threats, outcome dependence, a sense of powerlessness, political allegiance and alienation, and power of status quo as well as social stability to mitigate resistance and enhance the perceived legitimacy of the VCSL and the ruling regime.

This thesis contributes to the theoretical advancement of SJT by providing an institutional perspective and evidence of the system justification on public discourse, thus, offering a nuanced understanding of how authoritarian regimes utilize media rhetoric to shape public perception, maintain political stability, and legitimize controversial policies.

ACKNOWLEDGEMENTS

My Ph.D. was a joyful journey and has become an unforgettable piece of my adulthood. It had too little tears and fears but was overfilled with laughter and enlightening moments. In the past years, my life has been more meaningful and lively than ever before. I learned, I traveled, and I met new people. Every day, I walked on Hong Kong's streets knowing I was the happiest person on my own planet, the Moon.

Thanks to all my schoolmates, whom I see as friends for life. Being their friend is the greatest blessing anyone would ask for.

Special thanks to my supervisor-my Communist comrade, from whom I learned all about wisdom and inner peace just by looking at his attitudes toward life. I bet I could see him in Antarctica watching a Bee Gees show one day.

Thanks to all professors, course instructors, and supporting staff, who have always been a source of support and inspiration. I treasured each smile of theirs as I always felt care and sincerity in it.

And finally, thanks to Killer, without whom, the Hong Kong in me could never be this beautiful.

To Kyle and our political jokes,

Table of Contents

List of Tables

List of Charts

List of Firgures

List of Abbreviations

VCSL	Vietnam's Cybersecurity Law
VCP	Vietnam's Communist Party
SJT	System Justification Theory
CDA	Critical Discourse Analysis
CL	Corpus Linguistics
MPS	Ministry of Public Security
MND	Ministry of National Defense
MIC	Ministry of Information and Communication
CTFs	Cyber Task Forces
PIPL	Personal Information Protection Law
CCSL	Chinese Cybersecurity Law
BBC	British Broadcasting Company
VOA	Voice of America
RFA	Radio Free Asia
RFI	Radio France Internationale
CRI	China Radio International

Chapter 1. Introduction

The promulgation of Vietnam's Cybersecurity Law (hereafter VCSL) in 2018 has sparked extensive debate among the public and mass media, with supporters and dissenters expressing divergent views. Proponents, including lawmakers, supporters, and state-sponsored entities, argue that the law is a critical and timely institutionalization of the Vietnam Communist Party's (hereafter VCP) commitment to protecting national security and maintaining social order amidst increasing cyber threats and crimes (Nguyen & Bui, 2018). Conversely, dissenters, such as activists, human rights groups, and foreign media, criticize the law as an expansion of government surveillance into cyberspace, raising significant concerns about privacy and civil liberties, and potentially damaging the country's economic growth prospects (McKirdy, 2019). Thus, the enactment and enforcement of the law involves not only a propaganda process to inform the general public but also a struggle to maintain power, political stability, control dissent, and enhance legitimacy through justification strategies. Understanding these strategies employed by the party-state to legitimize such controversial laws is crucial.

The overarching purpose of this thesis is to examine the justification strategies employed by the Vietnamese party-state to legitimize the VCSL. This study is grounded in System Justification Theory (hereafter SJT), which posits that individuals have a cognitive and psychological need to perceive existing social, economic, and political systems as just, legitimate, and necessary, even if these systems disadvantage them. Traditionally, SJT has focused on bottom-up perspectives of individual psychological traits and beliefs. This study, however, extends the theoretical approach to an institutional or top-down level. By examining how narratives are crafted and disseminated through the mouthpiece of the party-state, state-sponsored media, this study contributes to a deeper understanding of how ruling actors deploy narratives to resonate with people's cognition and psychology, subsequently motivating them to justify the existing socio-political arrangement and the regime in general. This thesis consists of three studies, each addressing specific objectives.

The study employs a mixed-methods approach, combining qualitative and quantitative analyses to provide a comprehensive examination of state-sponsored media discourse on the VCSL. Critical Discourse Analysis (hereafter CDA) is used to explore how language and framing shape public perception and justify the law, while quantitative methods such as content analysis, keywords comparison, and topic modeling analysis offer insights into the prevalence and categorization of these narratives.

The research found that political leaders use narratives emphasizing imminent cyber threats, the persistent presence of hostile and reactionary forces, the powerlessness of internet users, and a pervasive sense of cyber vulnerability to heighten citizens' existential and relational needs for security and social cohesion. By focusing on these looming threats, leaders foster an atmosphere where citizens feel vulnerable and, therefore, more inclined to seek protection. In stark contrast to these threats, the party-state's leadership is portrayed as decisive, competent, and powerful, creating an inevitable dependence in which the state appears as the sole reliable safeguard against perceived dangers. This juxtaposition not only encourages citizens to feel a sense of dependence on the government but also fosters political allegiance, enhancing the legitimacy of the VCSL and the regime itself. Through this framing, the law is presented as a necessary, logical, and responsible response to address urgent threats in cyberspace, thereby reducing public resistance. Additionally, the study identifies key justification strategies: rationalization, moralization, authorization, denial of system shortcomings, and stereotyping/delegitimization. These tactics form a comprehensive ideological framework that reinforces the system's legitimacy while countering dissent. By rationalizing the VCSL as essential for national security, appealing to public reason and morality, enhancing credibility through authoritative figures and institutions, addressing potential criticisms, and undermining dissenting voices, the media foster a collective perception that existing social and political arrangements are just, legitimate, and indispensable. This multifaceted approach underscores how media discourse effectively constructs a narrative that validates state power, solidifies public compliance, and minimizes opposition, ultimately reinforcing system justification in Vietnam.

This study makes several significant contributions to SJT. First, it expands the scope of the theory by providing an institutional perspective for the system justification of a specific law, dedicating insights into broader political practices of the regime. Second, it highlights the critical role of language in forming justifications, demonstrating how state-sponsored media use language to construct and perpetuate ideological narratives. Third, it systematizes justification strategies, addressing a gap in SJT regarding how systems organize and develop ideologies into different justifications. Finally, the study employs both qualitative and quantitative methods, offering a richer and more nuanced understanding of how justification strategies are constructed and disseminated.

This thesis consists of 8 chapters including the Introduction and Conclusion chapter as the first and the last.

Chapter 1. Introduction

Chapter 2. Study background

This chapter outlines Vietnam's media system and internet governance, controlled by the VCP, and details the escalation of censorship. It introduces the VCSL, its objectives, controversies, and criticisms. The chapter emphasizes the party-state's approach to cybersecurity and the VCSL's controversies since its 2018 draft, highlighting the significance of the research topic.

Chapter 3. Literature review

This chapter reviews cybersecurity, focusing on state-centric and human-centric approaches, and threat politics. It highlights the securitization theory, which leads to stringent socio-political measures against perceived threats. Besides state-centric approach under the lense of securitization theory, the chapter also explores the human-centric approach, prioritizing well-being over national interests, and analyzes both perspectives. Applicability and critiques of the

two approaches are also discussed in this chapter. By comparing these approaches, the chapter aims to clarify the complexities of cybersecurity discourse in various socio-political contexts.

Chapter 4. Theoretical foundation

This chapter reviews the SJT, focusing on its theoretical foundations, cognitive and motivational processes, empirical applications, and legitimation through the lens of the theory. The chapter also extends SJT's scope from the psychological and individual levels to institutional contexts, particularly in authoritarian regimes where ruling actors have the power and means to influence public perception. Regarding the present study, the chapter outlines the research objectives and integration of the theory into the following studies.

Chapter 5. Media Presentation of Vietnam's Cybersecurity Law: A Comparative Approach with Corpus-Based Critical Discourse Analysis

This study seeks discursive and heuristic evidence of situational attributes for system justification motivation through the presentation of state-sponsored media on cybersecurity threats that endanger national security, network security, and the rights and interests of individuals and organizations. It undertakes a comparative analysis of discourses on cybersecurity and the VCSL as presented by national and international media outlets. The study investigates how cybersecurity is framed, which topics are chosen, and how the VCSL is positioned differently through language usage in national and international media discourses. This comparative approach captures the dynamic and reflexive nature of the linguistic constructions adopted by the two media actors, facilitating further investigation into the diversity and opposition inherent in their framing strategies.

Chapter 6. Positioning of Us, Them, and the Powerful Leadership of the Party-State

Study 2 expands Study 1's findings on antagonistic narratives between state and international media discourse. This study specifically deepens an analysis of the party-state's

stance and positioning of involved parties in state-sponsored media discourses, looking for evidence of dispositional attributes, analysing factors that contribute to cognitive motives for system justification through the positioning of powerless lay people in contrast to the unlawful hostile forces and the powerful party-state. This study also investigates an assignment of rights and obligations to relevant stakeholders, which served to satisfy the need for closure and orientation among lay people.

Chapter 7. System Justification Strategies of the VCSL in State-Sponsored Media

This study uses CDA to examine system justification strategies employed by the party-state and state media to legitimize the controversial cybersecurity law, including authorization, rationalization, moralization, denials of system shortcomings, and stereotyping or delegitimization. Through a comprehensive examination of the text and its context, this study reveals latent ideologies and justification strategies in the legitimization process of state and media actors.

Chapter 8. Conclusion

Chapter 2. Study Background

Introduction

This chapter provides a comprehensive social context for the study, detailing the main characteristics of the media system and state governance of the internet and social media across three distinct phases. It outlines Vietnam's approach to cybersecurity and introduces the objectives, controversies, and criticisms of the VCSL. The first section highlights the primary features of Vietnam's media system, which operates under a "socialist-oriented market economy" and is controlled by the VCP and relevant government bodies. This section sets the stage for the following section by illustrating the close connection between the media system structure and stringent media regulations, including the escalation of censorship over three generations of internet governance.

While the first two sections in this chapter provide a general overview of media and internet governance in the country, the final two sections delve into the party-state's approach to cybersecurity. These sections explain how the VCSL has become controversial since its draft introduction at the 14th Vietnam National Assembly in 2018. This chapter not only helps readers understand the context in which the study takes place but also emphasizes the significance of the research topic.

2.1. Newspapers and Media System in Vietnam

The Vietnamese press system operates under under the leadership of the VCP and the management of the State. According a statistics of Vietnam News Agency, by the end of 2023, there are 6 pivotal multimedia communication agencies (People Newspaper, VTV, VOV, Vietnam News Agency, People's Army Newspaper, People's Security Newspaper), 127 recognized press agencies, 671 magazine agencies, and 72 radio and television agencies owned by central and local governments, as well as other government bodies such as the Ministry of Information and Communication and Vietnam's Youth Federation. Privately-owned press

agencies, which are news outlets that not operated under government onwership or control either directly or through state-linked entities, are not recognized in the country.

The VCP exerts significant control over the media, and the government oversees all print and broadcast outlets. According to the Regulation No. 101/QD-TW in 2023, leaders of the press agencies or recognized news outlets, except for ones belonging to religious orgaizations, must be VCP members and have high-level political qualifications. Media content is strictly censored and controlled by the VCP and the Central Committee's Publicity and Education Commission. As stated in Article 4 of the 2016 Press Law, the media must serve as the mouthpiece of the party, state agencies, and other socio-political bodies. Private media are not officially recognized as distinct entities in successive Press Laws (Vietnam National Assembly, 2016; Yến-Khanh, Phelan, & Gray, 2022).

The Vietnamese government permits both non-permanent journalists and foreign correspondents to conduct press and information activities in the country. Although Decree 88 has been amended to ease procedures and requirements for foreign media, their activities remain under strict government oversight. For instance, under Article 13, permanent reporters must seek written approval from the People's Committee of centrally affiliated provinces and cities where they wish to conduct their press activities, and they can only perform their duties within those approved areas. Additionally, Article 17 stipulates that the publishing and circulation of foreign information publications must comply with the Press Law, Publication Law, and other relevant Vietnamese laws (Decree 88, 2012).

Nine foreign media outlets have Vietnamese-language news websites, including the British Broadcasting Company (BBC), Voice of America (VOA), Sputnik News, Radio France Internationale (RFI), Radio Free Asia (RFA), China Radio International (CRI), Radio Taiwan International (RTI), Radio Korea International (KBS World), and The Epoch Times (Đại Kỷ Nguyên). However, these websites are not always accessible. BBC, VOA, and RFA, for instance, are inaccessible in Vietnam without firewall add-ons. The accessibility of Sputnik News varies

depending on the current political climate, such as during Russia's attack on Ukraine (Accessed on 1 March 2022). Access to these foreign media websites also depends on the policies of internet and data service providers. The restricted accessibility relates to the country's heavy internet censorship, primarily targeting overseas political opposition, human rights, and religious issues that the Vietnamese government opposes (OpenNet Initiative, 2005).

While there is no explicit regulation, certain sensitive and taboo topics are highly censored and thus cannot be covered by any "official" media outlets. These include political pluralism, human rights and religious issues, critical reflections on the past (Sanko, 2016), regional comparisons (especially northern-southern issues), bureaucratic incompetence in preventing top-level corruption (McKinley, 2008), freedom of speech and assembly (Gillespie, 2014), land rights controversies (Abuza, 2015), and the relationship with China (Công Khế, 2014, as cited in Yến-Khanh, Phelanb, & Gray, 2022).

Vietnam consistently ranks at the bottom of worldwide press freedom indices, despite government denials of international accusations regarding violations of press freedom and freedom of speech. According to the World Press Freedom Index, from 2014 to 2021, Vietnam ranked as low as 175th out of 180 countries. The U.S. government-funded rights group, Freedom House, labels Vietnam's media environment as one of the harshest in Asia, and Human Rights Watch describes Vietnam as one of the most intolerant in the region.

2.2. State Governance of the Internet and Social Media

Similar to China, Vietnam employs various strategies to censor online content and regulate Internet users. The first generation of Internet control, initiated during the early stages of Internet adoption in the country, involved technical firewall interventions to block specific websites (Luong, 2022). In the 2000s, in response to the proliferation of websites and the government's limited management resources, the second generation of control emerged. This phase was characterized by a series of laws and regulations aimed at adjusting online behaviors and addressing "anti-state" activities. According to Luong (2022), from 2001 to 2005, during the

pre-Facebook era, the government issued seven Decisions and Directives prohibiting the use of Internet resources for storing military, economic, security, or other state secrets on Internet-connected computers to oppose the state or disturb social order.

The third generation of control began after the government failed to restrict Facebook following its arrival in 2006. This approach combined "hard" management, including new and strengthened regulations, with "soft" management strategies. Following the closure of Yahoo! 360, Facebook quickly attracted numerous users and became the most powerful social networking site. By 2021, Facebook had 76 million users, accounting for 76.7% of the population (World Population Review, 2022). Among platforms, Facebook has become the most effective means for navigating censorship and restrictions on information and critical knowledge (Bui, 2016). Initially, Facebook was intermittently banned as the Vietnamese government emulated China's strict Internet censorship. However, Vietnamese users found diferent ways to bypass government restrictions to access the platform including using VPNs and other browsers extensions and apps. Given the government's neutral stance in international relations with China and the U.S., blocking international social media services could negatively impact Vietnam's business environment with U.S. counterparts (Le, 2019). Consequently, the government relaxed its stance on Western platforms while continuing to enforce new laws and regulations on social media users. National media, newspapers, and other state-party bodies, including political elites, also used Facebook as an extended channel to strengthen propaganda and monitor public opinion.

In another attempt to control internet user mobility, the controversial Internet Decree on Management, Provision, and Use of Internet Services and Information Content Online took effect on September 1, 2013. Decree 72/2013-ND-CP prohibits using Internet services and online information to oppose the Socialist Republic of Vietnam, threaten national security, social order, and safety, sabotage national unity, arouse animosity among races and religions, or contradict national traditions. The Decree also targeted foreign organizations like Facebook, Google, and other cross-border public information suppliers to comply with Vietnam's law.

The Decree 72 was amended by the Decree No. 27/2018/ND-CP dated 1 March 2018 and Decree No. 150/2018/ND-CP dated 7 November 2018 to encourage users (including State authorities and officials) to use their real names on social network platforms, register their information for certification and contact, share information with official and reliable sources, share positive information about good people and good deeds, promote and advertise the country, people, beautiful cultural traditions of the Vietnamese people, educate and protect children and teenagers in cyberspace, and not to advertise or trade in illegal services. Targeting journalists, Decree No. 1131/QĐ-HNBVN issued on December 24, 2018 banned them from posting news, articles, images, sounds on social networks, making comments, sharing personal views or re-posting speeches and opinions that are contrary to the guidelines, guidelines and policies of the Party and State; contrary to the content and opinion of the journalistic work that the journalist himself has written and published, contrary to the opinion of the press agency where he or she works. In June 2021, the government continued to issue the Code of Conduct for Social Media under the Decision No. 874/QD-BTTTT. The Decision sets forth include respecting and complying with the law; having healthy behavior and conduct in line with the nation's good moral, cultural and traditional values; complying with regulations and instructions on information safety and security; taking responsibility for behaviors on social networks; and cooperating with competent authorities to handle acts and information content in violation of the law. The rules apply to service providers for having measures for detecting, notifying and coordinating with the State authorities to handle, prevent and remove content in violation of intellectual property and other laws and protect information of users, etc.

More importantly, the third control generation has been using “flooding” tactics by which government-sanctioned cyber troops are deployed to overwhelm social media platforms with mostly politically neutral and misleading messages (Luong, 2022). Similar to the “fifty-cent” cyber troops of China, the Force 47 in Vietnam is a 10,000-strong military cyber unit tasked to manipulate online discourse to enforce the Communist Party’s line (Hookway, 2017). On the one hand, these forces shape public opinion by sharing party-state messages and redirect news flow. On the other hand, the squads target and suspend accounts and content belonging to activists

(Bradshaw & Howard, 2019) by massively reporting their Facebook accounts as spam. While this co-option tactic is totally a loss to online activists, it is deemed a win-win situation to sort out constraints between Facebook's policy and the government's account block requests. Reported accounts will be suspended in silence for violating Facebook's community standards, making the process appear legitimate and not directly influenced by the government. The whole process, thus, is legitimate, as it is a result of the platform's content moderation for the public good rather than an output of governmental intervention. Consequently, Facebook trades user's free speech for market access in Vietnam, undermining the Internet's democratizing potential (Biddle, 2020).

The Vietnamese government's concerns and tightened censorship on social media stem from several factors. Firstly, the state does not own social media and has limited content control. While the government can censor news websites through domain management, it cannot block "illegitimate" and undesirable social media presence, such as those of BBC, VOA, RFA, RFI, and other international actors. Secondly, social media not only diverts readers from the conventional press, where the government strengthens propaganda to orient public opinion, but also influences public opinion by filling gaps left by mainstream media (Brown, 2015; Bui, 2016). Thirdly, social media enables like-minded users to connect, spread information quickly and cheaply, and nurture a public sphere in a country with limited freedom of expression. This increases the risk of toxic content, potential state secret leaks (Lam, 2022), and online activism that challenges government resilience and social stability. Notable online activism events that gained domestic and international attention include the "6700 people for 6700 trees" campaign in 2015 (Bui, 2016), the Formosa industrial toxic waste incident in 2016, and the Special Economic Zone bill protests in 2018 (Lam, 2022).

2.3. Party-state's Approach to Cybersecurity

Vietnam's approach to cybersecurity closely parallels that of China in many respects. As a socialist country, the ultimate purpose of the VCSL is not only to protect cybersecurity but also

to safeguard regime and national security. While Vietnam's cybersecurity legislation does not explicitly mention cyber sovereignty, its overall objective is “protecting national security and ensuring social order and safety in cyberspace; and the responsibilities of agencies, organizations, and individuals involved” (Vietnam's Cybersecurity Law, 2019). The law defines cybersecurity as “the assurance that activities in cyberspace will not cause harm to national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals.” A crucial aspect of Vietnam's political dynamics in cybersecurity governance is the alignment of policies with the state's overarching objectives (Thayer, 2020). The administration prioritizes social order, national security, and the power of the VCP (Vasishta & Kapoor, 2024). This socialist approach highlights the importance of addressing political and ideological threats to the stability of the socialist state, the hegemony of the communist party, and the legitimacy of Marxist-Leninist ideology (Bui & Lee, 2022).

Cybersecurity laws in Vietnam, under the principles of socialist legality, are enacted and interpreted by political and governmental bodies to facilitate state intervention in controlling socio-economic activities and citizens’s behavior in cyberspace through stringent regulations. These include content filtering, authorities’ access to personal data, banned activities, and data localization. The cybersecurity law typically lists banned acts in vague language to provide flexibility, allowing for responses to local conditions (Keller, 1994) or unexpected societal developments (Ross & Ross, 2000), and subject to broad interpretation by regulatory authorities (Lee, 2018) thereby encouraging self-censorship (Bui & Lee, 2022).

Within the cybersecurity regulatory framework, only state actors are responsible for implementing the VCSL. In Vietnam, the primary institutions involved include the government, the Ministry of Public Security (hereafter MPS), the Ministry of National Defense (hereafter MND), the Ministry of Information and Communications (hereafter MIC), and the Government Cipher Committee. Specific institutions include Cyber Task Forces (CTFs) under ministerial bodies.Vietnam's National Cybersecurity Strategy aims to strengthen state management of cybersecurity, complete legal frameworks, and protect national sovereignty in cyberspace. It also

seeks to develop a national coding infrastructure to protect national secrets and critical intelligence. A four-layer protection model is encouraged for critical information infrastructure, with "Made in Vietnam" technologies prioritized to protect national systems (Le, 2024). This model involves an in-house team (first layer), 24/7 cybersecurity services by a professional provider (second layer), an independent security audit (third layer), and independent monitoring by the National Cybersecurity Center (forth layer) (Scobell, 2023).

2.4. Vietnam's Cybersecurity Law: Objectives, Controversies, and Criticism

The VCSL took effect on January 01, 2019, after being passed at the 14th Vietnam National Assembly on June 12, 2018. It consists of seven chapters and 43 articles that regulate behaviors and responsibilities of agencies, organizations, and individuals in cyberspace with the aim of safeguarding national security and ensuring social order and safety. The law is designed to reinforce the country's cybersecurity network by providing more stringent protection of national information infrastructure, personal information, and online crime prevention. The VCSL encompasses several essential regulations such as data localization, collaboration between the government and telecommunications companies and internet service providers regarding personal data for investigation purposes, controlling the generation and dissemination of false news, content removal at the request of the government, and child protection in cyberspace.

According to Le Thi Thu Hang, spokesperson for the Ministry of Foreign Affairs, the VCSL represents an attempt to enhance security in the online environment that has encountered multiple challenges over the years, especially due to the absence of a legal framework and cybersecurity assurance capabilities (Nguyen Manh Hung, 2018). The VCP has emphasized that the law is aimed at protecting the legitimate rights and interests of all citizens and organizations, ensuring the stable development of Vietnam, and conforming to international law (Thai, 2018).

Despite being passed with 87% of the votes at the 14th National Assembly, the law has been a subject of controversy, opposition, and criticism (Nguyen-Thu, 2018). The law has been criticized for increasing "a totalitarian model of information control" (Bates, 2004), violating

human rights, and creating barriers to business (Nikkei Asia, 2018). Activists, human rights groups, and foreign media have accused the Vietnamese government of using the law as a means to instrumentalize political ideology to surveil citizens, target online dissidents, suppress revelations of government wrongdoing, and quell political mobility and online activism (Nguyen et al., 2022).

While the VCP's politburo affirmed that the VCSL was modeled after similar laws in developed nations such as the U.S., the U.K., Australia, Japan, Singapore, and Korea, many believed that it primarily followed in the footsteps of the country's counterpart, China (Sherman, 2019), by creating a draconian cybersecurity law aimed at strengthening the authoritarian regime and maintaining political security, rather than promoting cyberspace protection (AFP, 2019). Consequently, the law has been viewed as a new step in the consolidation of secrecy and political stability (Tran, 2020) and has been heavily criticized for exacerbating the country's already-poor internet freedom and political status quo.

Some of the controversial regulations in the VCSL include data localization and local office requirements, personal data verification, and data provision upon government request for investigations into illegal content creation and dissemination, as well as suspension of social media accounts and content removal within 24 hours for certain types of information deemed detrimental to public order and political stability. While the government's surveillance of online content and personal data raises concerns about personal privacy, the data localization requirements and regulations on cross-border transfer of personal data have been criticized for harming the business-friendly environment in the country. As a consequence, these stringent regulations would fail to leverage its digital economy (Viet, 2021).

To be more specific, both national and international public heavily criticize the law as it raises at least three critical issues.

First, new regulations under Article 26 on information and data management violate Internet users' privacy as the government has access and full control over user data with the

authority to request service providers to take actions on blocking or suspending user accounts that are deemed to violate the law within 24 hours. In order to comply with the law, from June 2018 to June 2021, YouTube removed thousands of videos, which mainly contained criticism content towards the party-state, upon 875 requests from the government (Google Transparency Report, 2021). Meanwhile, the number of similar contents being removed before the VCSL's promulgation from 2014 to 2017 was just 60. More critically, a working group was also established between Facebook and the Ministry of Information and Communications to identify and handle content violations on that platform (Sen, 2019). Under the collaboration, in 2019, Facebook scrapped 200 embedded websites with anti-governmental content, 208 fake accounts, and 2,444 websites that promoted sales of "illegal products and services" (VnExpress, 2019). In 2020, the Vietnam government threatened to shut down Facebook in the country if the company refused to censor more political and sensitive content (Pearson, 2020). Therefore, the giant tech company, in 2020 alone, complied with 95% of the content removal requests from the government (Cloud & Bengali, 2020), and increased the amount of content with restricted access in Vietnam by over 500% in the last half of 2018 (Reuters, 2019).

Second, closely related to data management issues is public concern about the violation of freedom of expression, freedom of speech, access to information, freedom of opinion, and other rights relating to political interests, according to Human Rights Watch (Russin & Vecchi, 2021). Article 8 and Article 18 prescribe prohibited acts in cyberspace that cover "propagation against the Socialist Republic of Vietnam; inciting riots, disrupting security and public order; personal humiliation and slander and so on..." The law aims to strengthen the Penal Code by extending governmental surveillance to cyberspace to handle independent or "left-sided" journalists and bloggers who "making, storing, disseminating or propagandizing information, materials, and products that aim to oppose the State of the Socialist Republic of Vietnam" (Penal Code, Article 117) and "abusing democratic freedom" under Article 331. These are vague but familiar regulations that the government normally used to put many activists and journalists in jail in the past years (Nguyen, Bui, & Phung, 2022). By the end of 2021, 43 journalists have been imprisoned under the new law (Reporters Without Borders, 2021). The imprisonment of

journalists and bloggers seems to be a classic tactic of "kill one to warn one hundred" in authoritarian countries (Cain, 2014). The law has forever changed the online environment, which used to be considered as an open space for political discussion and activism. The linkage to the Penal Code and increasing presence of the Ministry of Public Security has also proved to have negative impacts on the public's willingness to participate in grassroots collective actions or to voice their discontentment towards policy issues such as signing petitions to the government, sharing citizen's concerns on social media, and joining street protests (Truong, 2024). Overall, the law infringes four rights, which are privacy, freedom of expression, the right to use telecommunication services, and the right to benefit from ICT and social networks (Savenet, 2019, pp. 77-78).

Third, following the general data localization requirement under the VCSL, Decree 53/2022/ND-CP (Decree 53) with more detailed measures on storage and local presence requirements that came into force on October 1, 2022. Foreign enterprises in certain business and service sectors such as telecom, e-commerce, online payment, social networking and social media… are required to set up a representative office or branch in the country. In addition, both relevant domestic and foreign must store certain types of data for a minimum of 24 months upon request. The new requirements have worried many that they will discourage foreign companies from investing in Vietnam due to extra costs and complicated operation procedures, as well as challenge the country's commitment and obligations in international agreements such as CPTPP and RCEP (Fox, 2023).

The enactment of the VCSL is believed to establish a digital ecosystem that is independent of the global arena, with the aim of exercising greater control and oversight over "toxic content" (Sherman, 2019). While these measures have been criticized as heavy-handed, they are ultimately aimed at criminalizing unlawful activities and safeguarding the interests of dominant state actors (Neo, 2022).

Chapter 3. Literature Review

Introduction

This chapter provides an in-depth review of existing cybersecurity literature, focusing on two main approaches to understanding and conceptualizing cybersecurity. First, it introduces the predominant state-centric approach with the key concept of hypersecuritization, highlighting how cybersecurity measures are often framed around national security and political sovereignty, particularly in the context of securitization theory. This theory, a cornerstone in security studies, underscores how states frame cybersecurity as a national security issue to mobilize political goals and justify restrictive socio-political measures to counter perceived existential threats. Second, the chapter explores the emerging human-centric approach, which contrasts the state-centric perspective by prioritizing individual rights, well-being, and digital security over state interests. This approach, rooted in neoliberal thought, redefines cybersecurity as a collective responsibility shared by governments, private sector entities, and civil society, placing greater emphasis on privacy, freedom of expression, and protection from state surveillance. Criticism of both approaches is also discussed in this chapter.

In addition to these theoretical perspectives, the chapter also examines "threat politics" in media discourse. Media narratives often amplify the perception of cyber threats, portraying them in ways that bolster state-led initiatives while shaping public opinion to favor security over personal freedoms. This section highlights how Western and Asian countries employs threat-based media discourse to legitimize extensive cybersecurity measures by framing them as essential for societal protection and contributing to the normalization of state control in cyberspace. The chapter also discusses consequences of the overemphasis on cyber threats on media. Associating with threat politics, the chapter highlights legitimation discourse around cybersecurity in authoritarian context, citing how the regimes exaggerate threats to justify measures and government surveillance under the name of protecting national security and social order.

By consolidating these perspectives, the chapter aims to provide a nuanced understanding of the complex interplay between cybersecurity policies, state interests, human rights, and media influence. This comparative framework reveals how different socio-political contexts shape cybersecurity narratives, illustrating the ongoing tension between state sovereignty and individual freedoms. Through this comprehensive review, the chapter establishes a theoretical foundation for analyzing how these competing discourses impact both national cybersecurity policies and public attitudes, setting the stage for further exploration of cybersecurity's role in contemporary governance.

3.1. Defining Cybersecurity

Cybersecurity is a variable, context-bound, subjective, and sometimes, uninformative (Craigen et al., 2014), overlapping, and contradictory (Shires, 2020) concept. The notion of cybersecurity does not adhere to a singular viewpoint as there are multiple interlocking discourses around it (Cavelty, 2010). This concept is socially constructed by securitizing actors (e.g., state and the government) (Buzan et al., 1998), who define security and shape responses to envisaged threats (Stritzel , 2007) on hypothetical scenarios or what might be rather than on current realities or what is happening. Consequently, cybersecurity can be regarded as a matter of constituting discourses, rather than a pursuit aimed at hunting down real threats and apprehending actual culprits, as guilt is often presumed rather than proven (Sangbae, 2014).

Despite the absence of a widely accepted and all-encompassing definition of cybersecurity, most scholars argued that there are two main approaches to defining the concept: the technical approach and the national security approach.

The technical aspect places cybersecurity as the body of technologies, processes, and practices to protect confidentiality, integrity, and availability (CIA model) of information network and data (Cavelty, 2019). Within this framework, the definition of cybersecurity focuses on information infrastructure and system vulnerabilities, technical-related threats (such as equipment failure, denial of service, unauthorized accesses, and breaches of user privacy and

data confidentiality…), and the risks associated with malicious attacks that compromise confidentiality, integrity, or availability (Craigen et al., 2014; Lezzi, Lazoi, & Corallo., 2018).

Meanwhile, the national security perspective conceptualizes cybersecurity from understanding of (normally) state actors about potential cyber threats and encroachments on national sovereignty (Górka, 2021) to justify their political intervention in both domestic and international affairs. From a state-interventionist standpoint, the protection of cyberspace, as an extension of territorial sovereignty, is deemed legitimate, often leading to the framing of cybersecurity as a military issue (Górka, 2021). In this framework, cybersecurity is a necessary resort at the national level to secure political stability through measures such as censorship and regulatory controls that may restrict press freedom (Sangbea, 2013).

Cyber sovereignty is an institutionalized product of the state-centric approach. The idea of cyber sovereignty, which is derived from the concept sovereignty, has been propagated by China and its counterpart, Russia, to imply supreme authority within a given territory (Philpott, 2020) over citizens and subjects, unrestrained by the laws (Dunning, 1986), and to justify practices deemed unacceptable in many democracies, such as tight control of internet gateways or the censorship of political content online (Sherman, 2019). Cyberspace, thus, is treated as any physical territory; and within that fixed boundary, one authority devises rules, laws, norms, and behavior of individuals, organizations, applications, and other actors and factors (Mirza, Ali, & Qaisrani, 2021).

According to Yeli (2017), with the cyber sovereignty concept, there are three disputes among three main actors in cyberspace (state, citizens, and international community) including contradiction with the unrestricted interconnectivity or the spirit of the internet (between state and international community), contradiction with human rights in the tensions free flow of information and freedom of speech (between the state and citizens), and contradiction with the involvement of multiple stakeholders in governance (between state, citizens, and international community). The approach, therefore, has been criticized due to the promotion of protectionism

(Shahbaz et al., 2020) or paternalism in the cyberspace and exploitation of the ambiguity of the sovereignty concept to interpret and propagate the meaning that suits state's interests (Palaniappan, 2022). The outcomes of these ideologies are data localization, nationalization, fragmentation of the internet, internet censorship, human rights violations, and many more.

The notion of cybersecurity as a component of national security derives from securitization theory, which posits that security is a process of identifying, understanding, and responding to cyber threats. This process involves the identification of security actors, the determination of securitized referent objects, and an assessment of the impact posed by the threat (Buzan, 1998). Despite the increasing criticism of the national security approach to cybersecurity (Lindvall, 2020), it remains the prevailing and predominant approach adopted by numerous countries. A more detailed elaboration of the dominance of securitization discourse on mass media will be further discussed in the next part.

In addition to the two above-mentioned approaches, there has been an emergence of the third approach, the human-centric or human security approach. It is grounded in neo-liberal discourse with a strong emphasis on freedom, openness, trust, and the free flow of information in cyberspace. The approach adopts a decentralized multistakeholderism perspective, predominantly led by the U.S. and other Western countries. It promotes the notion of cybersecurity as a shared responsibility among various actors, including civil society, the private sector, governments, academic and research communities, and national and international organizations to protect computer and network systems from cyber theft of proprietary commercial data or information (Sangbae, 2014) as well as other cyber attacks against the free flow of the Internet. At its core, the approach prioritizes individual-level security concerns, encompassing the protection of privacy, human rights, and freedom of expression (Górka, 2021) from state surveillance and information control (Deibert et al., 2011). It recognizes the significance of addressing cybersecurity in a manner that upholds and safeguards the well-being and rights of individuals.

The brief introduction above is to illustrate the contextual nature of the cybersecurity definition, which is contingent upon the perspective of the actor constructing the conceptual framework and emphasizing particular threats within the said definition (Górka, 2021). Furthermore, it is noteworthy to acknowledge that the dynamics of security politics function differently within non-democratic, often authoritarian, and illiberal environments (Zeng, 2021). Therefore, instead of looking for a ubiquitous definition of cybersecurity, Cavelty (2010) underscored the necessity of considering the contextual factors and conditions that influence the subjective process by which key actors collectively develop a shared comprehension of how to conceptualize and, ultimately, address a security threat (Cavelty, 2010).

3.2. State-centric Versus Human-centric Approach to Cybersecurity

As the technical perspective on cybersecurity is not the focus of this study, this section aims to introduce two main human-related approaches to cybersecurity: the securitization theory representing the state-centric approach and human security representing the human-centric approach.

State-centric Approach or Securitization Theory

Theory Overview

The securitization theory, representing the state-centric approach to cybersecurity, was initiated by Ole Wæver and further developed by Barry Buzan. Adopting a constructivist approach, they view security as a socially constructed discursive modality with particular rhetorical structures, political effects, and power dynamics (Hansen & Nissembaum, 2009) revolving around "threat politics" (Cavelty, 2007). Securitization, therefore, is the rhetorical act by which a political issue is articulated as an existential threat (Barnard-Wills & Ashenden, 2012), thus gaining public consent and enabling the authority to use whatever means it deems appropriate (Balzacq, 2011, p. 3). Due to the uneven distribution of power, cyberspace intersects

with state power, control, and order (Cavelty, 2007), with the state as the dominant actor in making interference and regulation.

Balzacq defines securitization as "an articulated assemblage of practices whereby heuristic artefacts (metaphors, policy tools, image repertoires, analogies, stereotypes, emotions, etc.) are contextually mobilized by a securitizing actor, who works to prompt an audience to build a coherent network of implications (feelings, sensations, thoughts, and intuitions) about the critical vulnerability of a referent object, that concurs with the securitizing actor's reasons for choices and actions, by investing the referent subject with such an aura of unprecedented threatening complexion that a customized policy must be immediately undertaken to block it" (Balzacq, 2011). A successful securitization implicates the tolerance of such a threat and the implementation of special measures; however, it does not need to convince the entire population of the existential threat if it captures powerful and influential groups (Emmers, 2007). Securitization combines the politics of threat design with threat management (Balzacq, 2011) and the interaction between power holders or threat designers and their audiences (Balzacq, Léonard, & Ruzicka, 2016). Hypersecuritization, or the securitization of exaggerated threats, is a key concept of the theory.

The securitization process involves developing strategies to address and challenge the "exceptional" status of security issues. An issue, even if it pertains to an individual matter, might be framed as "exceptional" due to its perceived threat to national interests or the specialized technical knowledge required to evaluate the threat. This framing elevates the issue to a higher level of urgency and significance, justifying extraordinary measures and policies. Securitization frames threats in terms of urgency, emergency, and survival, making security policy unique and placing it outside normal politics or military affairs (Wæver, 2010). The issue is then shifted from the domain of normal politics to the domain of crisis politics, where it can be addressed swiftly and without adherence to the usual (democratic) rules and regulations of policy-making (Wæver, 2004).

Cybersecurity, as an extension of traditional security in cyberspace and a critical concern for governments worldwide, has been mainly addressed from a top-down or state-centric approach due to its political significance. This approach emphasizes the role of state actors in securing national security and critical infrastructure through extraordinary security measures in response to cyber threats. Cyber discourse, therefore, depends on the socio-political context and always implies notions of power, domination, and control (Górka, 2023).

A powerful securitization discourse necessitates a dual shift out of the political realm: from the politicized to the securitized, and from the political to the technified (Hansen & Nissenbaum, 2018). When an issue is securitized, it transitions from standard political procedures to the realm of security, taking precedence over other issues and permitting extraordinary measures that would not typically be acceptable (Buzan et al., 1998, pp. 21–22). Securitizing an issue facilitates the justification of specific activities, initiatives, and policies while overriding other concerns, including ethical and societal considerations (Fichtner, 2018).

Securitization, based on threat-based security logic, implies the intent of conflicting parties, external threats to a referent object, and policy prescriptions focused on defence against direct causes of harm (Backman, 2022). It also implies a broader discourse on geopolitics and international relations with offensive and defensive cybersecurity and cyberwar strategies. In Western narratives, various types of digital danger emerge from the "non-West": terrorists using the internet for radicalization, devious hackers from North Korea, and high-tech surveillance techniques in China (Lacy & Prince, 2018). Conversely, in the Asian context, especially in China, the US is portrayed as a threat not just to the military but also to regime stability and communist ideology. Due to the dominance of securitization, the global discourse on cybersecurity is filled with uncertainty, risk perception, securitization, and potential militarization (Barnard-Wills & Ashenden, 2012).

Securitization is used by political leaders for various purposes: establishing a hierarchy of political priorities, deterrence, legitimizing past actions, introducing social control, preserving

the status quo, and defining one's own identity of 'self' in opposition to 'other' (Vuori, 2008, p. 69).

The theory constructs securitization into five main elements.

The first element, securitizing actors, refers to the agent who presents an issue as a threat through a securitizing move or speech act, that "by saying the words, something is done," (Buzan et al., 1998: 26) normally are the government, political leader, or military who has access to resources, control over discourse, and institutional authority, especially in an authoritarian context.

The second element, the referent subjects, is an entity that is threatening.

The third element, the referent object, is the entity that is threatened or "seen to be existentially threatened and that has a legitimation claim to survival" (Buzan et al., 1998). National security, sovereignty, critical infrastructure, and human rights are the utmost important reference objects that are securitized in both Western and non-Western contexts (e.g., Cheng, Pei, & Danesi, 2019; Luiijf, Besseling, Spoelstra, & De Graaf, 2013). The construction of referent objects depends on state's approach to security matters, subsequently framing security issues and influencing both security measures and the target audience's responses to securitizing moves.

The forth element, the audience, is the target either in formal or moral aspect (Balzacq, 2005), that needs to be persuaded that the referent object is existentially threatened (Buzan et al., 1998). The formal audience is the entity that must be persuaded of the necessity to take action. It provides formal support for the action, and without this support, no action can proceed. In a democratic context, this audience often consists of legislatures, as government actions such as the deployment of military forces require their approval. The second type of audience is the moral audience, which offers moral support for the securitization process. Their perspectives help shape the perceived legitimacy and ethical definitions of security (Baysal, 2020).

The fifth element is the context and the adoption of distinctive policies (Balzacq et al., 2016).

Hypersecuritization

Hypersecuritization is considered the presentation of "large-scale, complex, cascading disaster scenarios" (Hansen & Nissenbaum, 2009) and a "tendency to exaggerate threats and to resort to excessive countermeasures" (Buzan, 2004). These definitions reflect three characteristics of threat construction, which as large scale, cascading nature and their hypothetical and unpredictable outcomes (Hersee, 2019).

Large-scale threats refer to incidents that trigger the highest level of security concerns such as terrorism, cyber attacks that target national security, critical infrastructure, economic stability or democracy in general, and weapon proliferation. The digital realist positions the social realm in the hypersecuritization of digital disaster and catastrophe with a possibility of cyber war (Lacy & Prince, 2018), in which cyberspace is instrumented for espionage, sabotage and subversion (Rid, 2013).

Cascading security threats or cascading failure refers to a chain reaction or domino effect, in which, one security threat can exacerbate other issues, and the collapse of a component can lead to the collapse of another or even an entire system in the interconnected networks. Critically, consequences of cyber threats are not limited to cyberspace but also have real-life impacts that causes "societal, financial, military break-down, hence bringing in all other referent objects and sectors" (Hansen & Nissenbaum, 2009). For example, attacks on cyberspace might cause cascading failure of interdependent critical infrastructure such as Secure water treatment plant and a Water Distribution System (Palleti et al., 2021). The opposite direction of the cascading effect from damage and disruption in physical infrastructures to cyber infrastructure is also true. For instance, a natural disaster is projected to affect massive amounts of critical infrastructure data that are geographically and logically disparate (Kopylec, D'Amico, & Goodall, 2008). Cascading failure not only happens between tangible systems like cyber or

physical infrastructures but also transforms into fear and uncertainty among citizens and ends up in increased control, surveillance, restrictions as well as increasing armraces among nations.

The hypothetical characteristic of hypersecuritization refers to the potential, imagined, assumptive consequences of extreme threats. Security measures are built on the preemptive or preventive actions to the protection or anticipation of certain threats. This can be seen in the use of modal verbs *will, could*, and *would* in securitization discourse. Cyber-doom scenarios with exaggeration of threats and cautionary tales result in exaggerated consequences or hypothetical cascading failure as mentioned above, most frequently, are the mass collapse of critical infrastructures leading to serious economic losses, or civilizational collapse (Lawson, 2011). However, these imagined scenarios, have not been recorded in history or materialized, not even in part (Cavelty, 2010), but still largely in the domain of our imagination (Boer, Lodder, 2012).

The real-life consequences of relying solely on a hypersecuritization approach are profound. The securitization process tends to exaggerate threats rather than addressing risks concerning national security, digital sovereignty, and critical infrastructure, which fosters uncertainty and rivalry in international relations. Threat assessment in this context is not based on a critical analysis of the consequences of cyberattacks, technological developments, or potential defensive measures. Instead, it relies on a creative imagination of "what might happen if governments are not prepared" (Lawson, 2001). This results in heightened tensions between nations, increased militarization of cyberspace, and the proliferation of defensive and offensive cyber capabilities, leading to an arms race in the cyber domain.

Human-centric Approach or Human Security

While the securitization approach to cybersecurity is criticized for overemphasizing state narratives of national security and digital sovereignty, there has been a growing emphasis on a human-centric approach. This approach aims to reduce cybersecurity-induced friction and control while prioritizing human security as the primary referent object, understanding human behaviors, needs, and preferences (Gaur, 2023). It challenges the state-centric approach by

shifting the reference object of security from states to individuals (Kerr, 2010). The approach seeks to resolve the dilemma between national security and human security, which traps citizens in the "liberty versus security" conflict (Liaropoulos, 2016). It moves towards a socio-cognitive-technical direction that considers both inward-looking systems designed to protect users and organizations, and outward-looking human factors, including cognitive biases, behavioral patterns, and psychological needs (Grobler, Gaire, & Nepal, 2021).

A human-centric approach to cybersecurity revolves around three main domains: users, usage, and usability (Grobler et al., 2021). By focusing on users and accounting for differences in culture, situational awareness, personal experiences, psychology, behavior, and cognitive factors, this approach promotes security mechanisms that enhance user resilience (including education and training) and fulfil human needs such as autonomy, competence, security, and stimulation. Cybersecurity policies should not merely play a defensive role but also facilitate human well-being and empower people to face cyber threats fearlessly while respecting others' human rights (Kovacs & Hawtin, 2013).

Regarding usage, the human-centric approach advocates for cybersecurity systems that are user-friendly and transparent, improving the effectiveness of technical measures. Such systems should be secured by multi-jurisdictional legislative instruments against cybercrimes while being transparent enough to make users feel safe and secure. This aligns with the United Nations (UN) Development Programme's framework of achieving human security with "freedom from fear," "freedom from want," and "freedom to live in dignity" (Owiny, 2022). Enhancing usability through user compliance and effective interaction with the technology ecosystem is also a key objective (Grobler et al., 2021). The so-called user well-being in cyberspace aims to protect individuals from risks posed by both state and non-state actors, as well as from a state's negligence or premeditated actions against its own citizens (Kumar, 2021). Although the state is sometimes criticized as a source of endangerment to human security, the human-centric approach does not reject the role of the state in providing and facilitating security for its people (Hama, 2017).

From the position of securitizing actors, the human-centric approach requires a narrative transformation away from state-centrism, military, and war discourse, towards facilitating human disarmament with a focus on the inclusivity of non-state actors (Pytlak, 2023). This means re-centralizing individuals and their communities into existing cybersecurity discourses (Klein & Hossain, 2020). Cybersecurity practices under this approach require states to uphold their human rights obligations when developing and implementing cybersecurity measures and to commit to responsible state behavior in cyberspace (Pavlova, 2020). The outcomes of this approach can significantly influence global cybersecurity trends and policies, with far-reaching implications for human rights worldwide.

Despite its ideal nature, the human-centric approach is still primarily theoretical and not widely implemented, with exceptions such as the Japanese and Canadian governments adopting human security in their policy-making discourse (Hama, 2017). The approach is theoretically ambitious, attempting to include everything within the conceptualization of human security, which in reality can dilute its meaning (Buzan, 1997). Conceptually, it lacks a clear definition of human security, often confusing narrow conceptions of human rights with broader definitions of human development (Shepherd, 2013). Deriving from liberal democratic theory, the School of Rights and Rule of Law emphasizes threats arising from the denial of fundamental rights and the lack of the rule of law (Hampson et al., 2001). Meanwhile, the United Nations Development Programme (UNDP) in 1994 argued that human security in cyberspace should include community security, political security, and more narrowly, freedom from fear and repression. Other scholars extend human security to contemporary issues such as terrorism, small arms, and inhumane weapons (Dodds & Pippard, 2013).

Practically, cyberspace governance is still evolving, with stand-alone securitizing actors or alliances rather than a universal forum responsible for regulating global activities and protecting human rights (Liaropoulos, 2016). This situation perpetuates a cycle of security-insecurity, where actions by one country to secure its national security make other countries feel less secure, leading to further offensive-defensive measures (Liaropoulos, 2016). In the absence

of global governance, states become ubiquitous actors claiming to secure their citizens' needs, often justifying control and surveillance (Smith, 2010). Framing the protection of human rights in cyberspace as a national security issue can be counterproductive, potentially leading to abuses (Comninos & Seneque, 2014). For instance, banning encrypted messages can be seen as a violation of privacy and online anonymity, but can also be justified for national security reasons (Green & Rossini, 2015). The narrow perception of human security has historically been used to intervene in the internal affairs of developing countries and impose Western values, such as the US invasion of Iraq under the guise of human security (Hama, 2017).

Human-centric cybersecurity is often applied by non-government sectors at the micro level, such as businesses (Jamil et al., 2024), climate change initiatives (Klein & Hossain, 2020), and efforts to empower internet users in cyberspace through resource distribution, digital rights protection, government consultations on critical infrastructure, and citizen empowerment in policy-making processes (Kumar, 2021).

In summary, the differences between state-centric and human-centric approaches to cybersecurity lie in four main areas. First, the state-centric approach prioritizes national security and critical infrastructure, viewing humans as nodes in the network and part of the threat spectrum (Liaropoulos, 2016). The human-centric approach, however, places human impact at the center, considering threats from both state and non-state actors (Brown & Esterhuysen, 2017; Deibert, 2018). Second, the state-centric approach retains state actors as the main lawmakers, while the human-centric approach advocates for the inclusion of non-state actors and communities. Third, due to the differences in priorities and actors, while the state-centric approach results in aggressive, intrusive and defensive measures to protect national security, the human-centric approach encourages the development of a resilient system with peaceful practices for personal security. Forth, the vital distinction between the two approaches lies in their public discourse. While the state-centric approach requires strong rationalization and legitimation to justify control and restrictive measures, the human-centric approach upholds cooperative rhetoric to justify human rights standards and democratic governance.

3.3. Threats Politics in Media Discourse

Cyber-doom scenarios (Lawson, 2013), the depictions of state collapse, widespread injury, and death (Shires, 2020), are prevalent in cybersecurity discussions among experts, commentators, policymakers, and media discourse (Valeriano & Maness, 2015). Metaphors of military attacks, natural disasters, and nuclear weapons, such as the "cyber Pearl Harbour," (Clarke & Knake, 2010; Penetta, 2012) are frequently employed when discussing cybersecurity. The "threat politics" (Cavelty, 2007) emerges from the prominence of threats within the cybersecurity domain, and it is strongly context-sensitive and embedded in pre-existing social, economic, and political visions and realities (Creemers, 2023). The securitization discourse surrounding the information age often presents it as a catalyst for doom and destruction (Clarke & Knake, 2012).

The emphasis on cyber threats stems from securitization theory, as developed by the Copenhagen School. According to this theory, a particular fact, a person, or a development is signified as a danger to the military, political, economic, ecological, and/or social security of a political collective (Buzan et al., 1998). The establishment "the truth" about certain dangers (Huysmans, 2006; Léonard & Kaunert, 2011; Kingdon, 2003) that pose a potential threat to the survival of the state and its society (Tikk & Kerttunen, 2020) or a "reservoir of threat presentations"(Cavelty, 2013b) gives specific securitizing or "capable" actors in politics (Weldes & Saco, 1996; Campbell, 1998) with power and legitimacy to justify extraordinary responses and undemocratic procedures (Huysman, 2006; Wæver, 1995).

Security measures are not exceptional but routine processes in bureaucracies (Lobo-Guerrero , 2008) through establishment of dominant discourse patterns (Cavelty, 2013b). In the realm of cybersecurity, the notion of cyberterrorism, for instance, is viewed as a social construction, a product of meaning-making practices associated with political rhetoric and news media rather than an extra-discursive reality (Conway, 2008). This highlights the role of discursive practices in constructing and framing security threats. A successful securitization,

hence, is “a justification of the use of all available means to counter it including those outside the normal political rules of the game,” (Tikk & Kerttunen, 2020) such as permanent surveillance of populations, precautionary arrests of suspects, or pre-emptive invasions of foreign countries (Aradau & Munster, 2007).

The narrative of “cyber-noir” (Shires, 2020) constructed around cybersecurity serves as a framework for intervention, aiming to justify taking action (Creemers, 2023). In order to convince their audiences, lawmakers often emphasize the existence of an existential and imminent threat, allowing them to securitize the issue and justify deviating from standard procedures and established rules and protocols (Buzan et al., 1998).

However, the excessive news media use of the hazy definition of cyberterrorism can only feed the public with fears of the unknown (Keith, 2005) and encourage them to “be afraid, be very afraid” (Debrix, 2001). By perpetuating the seriousness of cyber threats, even those that have not yet materialized, the national discourse on cybersecurity is desirable for governments to suppress open discussions on Internet policy and instead focus on closed-door national security decision-making processes (Barnard-Wills & Ashenden, 2012), or to easily pass restrictive legislation that increases its power (Vegh, 2002).

For instance, a content analysis of cybersecurity discourse on the People’s Daily from 1994 to 2016 in China reveals a growing emphasis on military-diplomatic framing over time, with more than half of news directing cybersecurity threats to man-made reasons (Miao et al., 2019). This state’s cybersecurity discourse has resulted in the legitimization and legalization of various practices, including increased political censorship, unfair competition, assaults on infrastructure (such as the government's censorship of search results leading to Google's exit from the country in 2010), and Internet governance (as exemplified by President Xi's promotion of the concept of cyber sovereignty since 2015).

These issues hold significant implications for practical cyber politics (Lindsay, 2014). Furthermore, China's narratives surrounding cyber threats tend to be generic and ambiguous,

often amplifying the perception of threats without real events (Duckett et al., 2020). This ambiguity does not necessarily increase the individual perception of personal risk but instead fosters public skepticism and distrust in cybersecurity institutions and practices (Boholm, 2021). However, it also provides the government with greater regulatory power to address perceived violations and control behaviors related to cybersecurity.

It is noteworthy that not only totalitarian governments but also democratic states have been utilizing threat discourse and adopting measures like cyber-sovereignty to consolidate their power. This can be observed in the increasing government surveillance, censorship, and propaganda practices in democratic countries as well (Cavelty, 2014). However, the phenomenon of threat inflation, war framing, and a preoccupation with doomsday scenarios is often deemed unproductive and potentially counterproductive (Brito & Watkins, 2011; Lawson, 2013), and "could impair efforts to motivate appropriate policy responses to genuine cyber security threats" (Lawson et al., 2016).

Previous studies have highlighted the strong influence of U.S.-originated discourse on cybersecurity (Bolhom, 2021; Eriksson, 2001). This discourse focuses on identifying threats such as hackers, viruses, state-sanctioned espionage, and terrorism that target critical infrastructure (Cavelty, 2013; Hansen & Nissenbaum, 2009), intersecting with the realm of national security (Tikk & Kerttunen, 2020).

The prevalence of cyber-threat hype (Conway, 2008) has contributed to a rapid and abstract evolution of the threat landscape that comprises a cyber arms race (Dunn-Cavelty, 2019) and cyber warfare (Mello, 2020), especially after Russia attacks Estonia's networks in 2007 (Cavelty, 2019).

A study on U.S. media discourse on cybersecurity between 1991 and 2016 shows that the majority of news stories promoted the idea of possible and hypothetical "cyber Pearl Harbor," while only a few covered alternative perspectives (Lawson & Middleton, 2019). The authors also indicate that this discourse on information warfare has faced criticism from communication

scholars for its "concomitant weaponization of information and speech," (Lawson & Middleton, 2019) resulting in increasing blurry lines between legitimate public affairs and media manipulation and propaganda (Lawson & Middleton, 2019).

The excessive media attention given to the U.S.'s discourse on cybersecurity has spread horizontally "from mainly being an issue of relevance to the U.S. to the top of the threat list of more and more countries" despite fundamental differences in strategic contexts (Cavelty, 2012). Even the Chinese government has been influenced to use the West's experiences as a reference to reshape its relationship with society in cybersecurity and legitimize its control over cyberspace (Miao & Han, 2021).

A study on national cybersecurity strategies conducted by Luiijf, Besseling, and De Graaf (2013) shows that among 19 sampled countries, all of them acknowledged the existence of cyber threats (Ham et al., 2013). Specifically, 16 nations explicitly addressed these threats, while 14 countries incorporated them into their national security concerns (Ham et al., 2013). The authors further specified that, except for the U.S. and Japan, all nations recognized individuals, criminals, and organized crime as potential malicious threat actors. Additionally, thirteen countries identified the threat of hostile activities by foreign nations, while the same number of nations expressed concerns regarding (potential) cyber attacks by terrorists (Ham et al., 2013).

Another study conducted by Boholm (2021) analyzed 1,243 news articles published in Sweden between 1995 and 2019. The findings revealed the presence of 34 distinct threat themes, with approximately 98% of the articles discussing at least one threat. The study also observed a shift in focus over time, with earlier articles displaying more generalized attention towards cyber threats, while later articles tended to highlight specific incidents and events (Boholm, 2021).

Similarly, Jarvis et al. (2017) conducted a discursive analysis of 400 news media items on cyberterrorism, gathered from 31 media outlets across seven countries, spanning the period from 2008 to 2013. The results indicated that nearly 70% of the analyzed news items exhibited a distinctly "concerned" perspective on cyberterrorism, with an emphasis on its potential impact

on the state, critical infrastructure, and the private sector. In contrast, only 2% of the news items expressed a more skeptical view towards these threats (Jarvis et al., 2017).

In addition, a qualitative study by Sallinen (2020) on media discourse of the New York Times, Washington Post, and the Wall Street Journal in 2010 showed that cyber warfare was perceived as fear-provoking, revolutionary, and comparable to nuclear weapons in the United States (Sallinen, 2020). This study also indicated that although the words "combats" and "cyberwarfare" continued to carry strong connotations in news articles from these media organizations even after 10 years, cyberattacks and their seriousness had been normalized and downplayed in tone over time. Furthermore, there was a shift in news focus from national security and critical infrastructure protection in 2010 to cyber espionage in 2020 (Cavelty, 2019), with an increased emphasis on projecting the U.S.'s strong and secure identity on the world stage (Agius, 2019).

Cyber threats are diverse in terms of specificity, status, scale (Jarvis et al., 2017), and modality or mechanism through which something is perceived as a threat (Boholm, 2021). The first cluster of threats is primarily associated with technical aspects and vulnerabilities within information systems. The second cluster focuses on human-related threats with socio-political dimensions, including hackers, cyber criminals, cyber terrorists, cyber espionage, and cyber commands. These threats are characterized by their association with lawlessness and anonymity, highlighting the social and political implications of cyber attacks. The third cluster refers to catastrophic attacks on critical infrastructure that cause disruptions and cascading effects on civil defence, homeland security, or military operation (Cavelty, 2013). By categorizing cyber threats into these clusters, researchers aim to provide a comprehensive understanding of the different dimensions and manifestations of cybersecurity challenges.

Previous studies have highlighted that news reporting on cybersecurity tends to focus more on threats associated with human actors rather than technique-related threats such as phishing, spam, viruses, and malware. The dominant themes in news discourse revolve around

issues such as data breaches, national cybersecurity, cyber espionage, criminal hacking (Rader & Wash, 2015), cyberterrorism (Jarvis et al., 2015, 2017), and cybercrime (Wall, 2008). This discourse on cybersecurity primarily adopts a neo-positivist perspective, characterized by a cause-and-effect approach to justify the implementation of pre-emptive measures and strategies aimed at defending the state against cyber threats (Sallinen, 2020).

Based on the prevalence of securitization approach to cybersecurity, this study also places attention on the portrayal of cyber threats in media discourse. By studying the framing and presentation of cyber threats in state-sponsored media, this research aims to shed light on the discursive strategies employed by governments to legitimize the implementation of various cybersecurity practices in the VCSL.

3.4. Legitimation Discourse around Cybersecurity in Authoritarian Context

In authoritarian countries, the discourse surrounding cybersecurity often employs securitization as a means of legitimizing extensive control over digital spaces. This legitimation discourse justifies the imposition of stringent cybersecurity measures and surveillance under the guise of protecting national security and sovereignty. The rhetoric of securitization, which frames cybersecurity threats as existential dangers requiring extraordinary measures, is a central tool in this process (Balzacq, 2011).

Cybersecurity has become the central aspect of internet governance, which deals with the structural and infrastructural operation of the internet (Fichtner, 2018). The application of securitization theory and hypersecuritization originated in the U.S. and Europe and has been increasingly adopted in non-Western contexts. Within the Asian context, the Chinese discourse on securitization is the most well-studied. Securitization is examined within the broader scope of internet governance, cyber sovereignty, and cybersecurity discourse, or with specific focuses such as artificial intelligence (Zeng, 2021), fake news regulations, or military-diplomatic affairs (Miao, Xu, & Zhu, 2020)

Beyond the Chinese context, the concept of securitization is used to analyze cybersecurity discourse in the Asia-Pacific region (Segal et al., 2020), including in Korea (조원선, 2017), Indonesia (Ulum, 2017), and Kyrgyzstan (Wilkinson, 2007). It also contests the variation in fake news governance across the Asia-Pacific, including Thailand (Sombatpoonsiri, 2021), Indonesia (Lim, 2020), and Singapore (Teo, 2021).

The ongoing discourse on cybersecurity is problematic (Klein & Hossain, 2020), as it not only deemphasizes human needs and security but also allows states to justify cybersecurity policies and stringent regulations that victimize citizens. This approach leads to violations of freedom and human rights, turning citizens into victims of mass surveillance, or even a cyber arms race (Brantly, 2014).

As the nature of regulating cybersecurity is an "exaggerated securitization" (Thumfart, 2022), which aims to emphasize cyber threats to justify stringent regulations even when these conflict with other values, it raises questions on the legitimacy of securitization and legitimation of security initiatives, or which referent objects should be used to legitimize security measures. The traditional approach to securitization generally emphasizes the threats of the "inner enemy" (Schmitt, 2007), extraterritorial jurisdiction, thus mainly using national security and digital sovereignty to justify security measures without providing a clear referent object of security (Thumfart, 2022). Framing of existential threats is also the most dominant legitimation strategy as addressed in the previous section.

The development of legitimation discourse built in securitization theory has faced significant criticism. One major issue is that it does not reflect the diversity of cybersecurity discourses, but instead emphasizes the militarized, geopolitical perspectives adopted by some decision-makers, reinforcing a simplistic friend versus foe logic (Górka, 2023). Additionally, it oversimplifies the nature of securitization by reducing security matters to simple binaries, thereby making securitization an extreme version of politicization (Buzan et al., 1998).

Securitization and desecuritization are often viewed merely as processes of moving certain referent objects in or out of the realm of security through speech acts. Although the theory posits that securitization involves not only speech acts but also discursive politics and social processes, including interactions between securitizing actors and their audiences, and among the actors themselves (Nicimbikije, 2020), it tends to overemphasize the importance of speech acts as the sole instrument in the securitization process. This focus leads to another critique: the simplicity of empirical evidence for securitization, which is often studied and validated through discursive practices and narratives alone.

Another criticism lies in its state-centric approach, which portrays state actors as powerful rule-makers governing security matters while neglecting the role of non-state actors such as specialized institutions, media, and non-governmental organizations. Methodological and application-related critiques also arise. The discourse is often limited to traditional security contexts such as military and national security, lacking diversity in its analytical scope. Furthermore, the focus on speech acts constraints research methods predominantly to qualitative studies, case studies, and textual analysis.

Chapter 4. Theoretical Framework

Introduction

This chapter is divided into two sections. The first section provides a comprehensive review of the SJT, examining its theoretical foundations, key constructs, and empirical applications. This section delves into the cognitive and motivational processes that compel individuals to perceive the status quo as fair and legitimate, highlighting how these processes function to maintain societal stability (Jost et al., 2003). It will then synthesize legitimation and justification through the lens of SJT, analyzing situational and dispositional conditions under which the system justification tendency is strengthened.

In the second section, moving beyond individual level analyses, this chapter will introduce the theoretical rationale for extending SJT to institutional contexts. It will argue that understanding how political and social institutions craft narratives to reinforce the status quo is crucial, especially in authoritarian regimes where state-sponsored media plays a pivotal role in shaping public perception and maintaining control (Mai, 2019; Dukalskis & Gerschewski, 2017). By doing so, this study aims to fill the existing gap in SJT literature that has predominantly focused on bottom-up approaches.

The chapter will also outline the research objectives, which include examining how state-sponsored media in Vietnam presents cybersecurity threats, justifies the VCSL, and employs various ideological strategies to legitimize the law and its controversial regulations. Through a detailed analysis of media discourse, this study seeks to reveal the cognitive heuristics and psychological mechanisms that underpin the justification of political arrangements and highlight the interplay between individual cognitive processes and institutional narratives.

In summary, this chapter sets the stage for a nuanced understanding of the SJT, its application in authoritarian contexts, and the role of media in legitimizing state policies. By

providing a thorough literature review, it aims to elucidate the complexities of system justification and its implications for political legitimacy and societal stability.

4.1. System Justification Theory

Overview

SJT was initially formulated and developed by Jost and Banaji (1994), positing that individuals tend to defend, bolster, and justify aspects of the societal status quo despite their disadvantaged positions, operating at both non-conscious and conscious levels of awareness. Originally, the theory was built on concepts of dominance ideology and false consciousness, incorporating social psychological research on stereotyping, prejudice, and the internalization of inferiority (Jost, 2020c). Individuals are motivated to satisfy epistemic needs to reduce uncertainty and ambiguity, existential needs to assuage threat and insecurity, and relational needs to coordinate social relationships and achieve a sense of shared reality (Jost, 2019; Hennes et al., 2019). At the social level, individuals desire to see prevailing social systems as fair and just, making them more likely to affirm the goodness, legitimacy, and stability of these systems rather than challenge them (Jost, 2020c). Consequently, individuals remain loyal to existing social arrangements and political institutions, even when such structures produce unfavorable outcomes for them (e.g., Lind & Tyler, 1988).

Motivation for this tendency varies based on situational factors such as system threat, system inescapability and stability, or system dependence (Friesen et al., 2019) and dispositional factors such as powerlessness and low social status (Jost, 2020b), feelings of political alienation or allegiance (Cichocka & Jost, 2014), and need for order or openness to experience (Wang & Kobayashi, 2021).

SJT posits several antecedents to the motivation for justifying the status quo. Early versions of the theory identified several categories of antecedents such as cognitive, epistemic, motivational, and ideological factors (see Jost et al., 2003; Jost & Hunyady, 2005). Meanwhile,

more recent versions of system justification theory have expanded to include existential needs, such as the desire to manage threat, insecurity, and distress, as well as relational motives, including the desire to affiliate with similar others, coordinate social relationships, and establish a shared social reality (Jost et al., 2017).

The strongest form of system justification is also referred to as the status legitimacy hypothesis (Brandt, 2013), which predicts that low status groups will be more likely to legitimize social systems than high status groups (Owuamalam, 2018). This is driven by the motivation to reduce ideological and cognitive dissonance between one's situation and objective reality. Disadvantaged groups tend to use various cognitive heuristics to legitimize social systems, authorities, and outcomes. For instance, the poor in capitalist countries often justify the uneven distribution of economic resources (Haack & Sieweke, 2018), or women in male dominant societies persist in protecting social hierarchies (Bahamondes, Sibley, & Osborne, 2021; Vargas-Salfate et al., 2018). People are motivated to satisfy epistemic needs to reduce uncertainty and ambiguity, existential needs to assuage threat and insecurity, and relational needs to coordinate social relationships and achieve a sense of shared reality (Jost, 2019; Hennes et al., 2019). As a result, people need and want to see prevailing social systems as fair and just, and are more likely to affirm the system's goodness, legitimacy, and stability rather than challenge it (Jost, 2020c). SJT, in stark contrast to social identity theory, emphasizes out-group favoritism over in-group favoritism among disadvantaged group members (Jost, Banaji, & Nosek, 2004).

Empirical evidence has identified several cognitive processes in the system justification mechanism, including positive stereotypes towards high status groups and negative stereotypes towards low status groups (Stapel & Noordewier, 2011); complementary stereotypes such as "poor but honest" and "rich but dishonest" among disadvantaged people (Kay & Jost, 2003); and the palliative function of ideology, which enhances well-being by reducing the extent to which the disadvantaged see themselves or their group as targets of discrimination (Bahamondes et al., 2020) or boosting their sense of belongingness (Baumeister & Leary, 1995; Bahamondes et al., 2021). Ideological investment in political or religious institutions through rules, norms, and

guidance for individual conduct enables adherents to believe that they live in a society that is orderly, legitimate, and just (Cichocka & Jost, 2014).

The theory includes nine postulates.

i. People are motivated (often nonconsciously, without deliberate intention or awareness) to defend, justify, and bolster aspects of the status quo, including existing social, economic, and political institutions and arrangements.
ii. As is the case with all other motives in human psychology, the strength of system justification motivation and its expression are expected to vary according to situational (contextual) and dispositional (individual difference) factors.
iii. System justification motivation is activated or increased when (a) the system is criticized, challenged, or threatened; (b) the system is perceived as inevitable or inescapable; (c) the system is perceived as traditional or longstanding; or (d) the individual feels powerless or dependent on the system (and its authorities).
iv. System justification addresses basic epistemic motives to reduce uncertainty, existential motives to reduce threat, and relational motives to reduce social discord. Situational and dispositional variability in these underlying needs will affect the strength of system justification motivation.
v. There are several possible means by which the system can be justified, including direct endorsement of certain ideologies, the legitimation of institutions and authorities, denial or minimization of system problems or shortcomings, complementary stereotyping, and rationalization.
vi. For members of advantaged groups (or those who are favored by the status quo), system justification is consistent with self and group justification motives, and is therefore positively associated with self-esteem, in-group favoritism, and long-term psychological well-being.
vii. For members of disadvantaged groups (or those who are disfavored by the status quo), system justification conflicts with self and group justification motives, and

is therefore negatively associated with self-esteem, in-group favoritism, and long-term psychological well-being.

viii. System justification serves a palliative function. The endorsement of system-justifying beliefs and ideologies is associated in the short term with increased positive affect and decreased negative affect for members of advantaged and disadvantaged groups alike.

ix. Although system justification motivation typically leads people to resist social change (and to perceive it as potentially threatening to the status quo), people are more willing to embrace change when it is perceived as (a) inevitable or extremely likely to occur, or (b) congruent with the preservation of at least some aspects of the social system or its ideals.

Despite ongoing debates, according to the theory's founders, system justification occurs mostly at an unconscious level. The process is rather automatic and effortless due to the automaticity of ideology derived from conservatism, as well as unintentional learning on stereotypes and prejudice (Jost, Kay, & Thorisdottir, 2009). For example, empirical studies have found that in-group stereotypes derived from cultural ideas, such as negative attitudes toward immigrants and racial minorities (e.g., Kawakami et al., 2003), or discrimination towards Black people (e.g., Banaji, 2001; Blair, Judd, & Fallman, 2004), produce a priming effect without the individual's awareness of their influence (Bargh & Ferguson, 2000; Bargh & Chartrand, 1999). In another instance, exposure to national flags triggered nationalist ideology related to concepts of power, materialism culture, and aggression among Americans.

As the theory's literature has continued to grow, more empirical findings support the opposite argument that system justification is also a very conscious process. For example, perceived or subjective socioeconomic status (Li et al., 2020), sense of control (Yang et al., 2016), and perceived social mobility (Whyte & Han, 2008) positively correlated with system justification. In other studies, a sense of powerlessness was found to increase the legitimation of authority, thus fostering system justification (van der Toorn et al., 2015; Jost, 2020b). In another

study, perceived high threats to the system heightened emotional and cognitive responses that led individuals to retaliate against whistleblowers (Sumanth, Mayer, & Kay, 2011). Owuamalam (2018) argued that an unconscious system justification motive is theoretically inconsistent with the auxiliary cognitive dissonance propositions that SJT was built on. For dissonance effects to occur, the two opposing cognitions need to be cognitively accessible.

After nearly 30 years, despite inconsistencies in theoretical examination and debatable propositions, SJT remains a robust theory and has been examined in a wide range of social contexts. In a comprehensive review, Yang et al., (2019) proposed three explanations for these inconsistencies in the SJT literature including differences in the conceptualization of system justification and status-legitimacy; differences in moderator variables, including personal factors such as sense of control or perceived social mobility, social structures, and sociocultural factors such as freedom and equality or racial issues; and psychological mechanisms such as social identity, attention to intrinsic characteristics, or compensatory control.

Contextual Drivers of System Justification

System Threats

According to SJT, individuals are motivated to justify the socio-political systems they inhabit to satisfy epistemic, existential, and relational needs, a tendency that intensifies under threat conditions. In situations marked by threats such as terrorism, climate change, economic downturns, and natural disasters, individuals seek to bolster their perceptions and restore the legitimacy of the system to mitigate uncertainty, ambiguity, and insecurity (Friesen et al., 2019). Several psychological mechanisms underpin this phenomenon. First, in line with social identity theory, individuals act to restore their sense of worth in response to threats (Branscombe et al., 1999). Second, the palliative function of system justification fosters positive illusions (Taylor & Brown, 1988), reducing negative emotions, and enhancing feelings of belongingness and shared reality (Bahamondes et al., 2021). Third, according to terror management theory, humans

construct and adhere to cultural worldviews that imply order, permanence, and stability to avert existential terror, especially under conditions where mortality is salient (Ullrich & Cohrs, 2007).

The impact of threats on increasing the motivation for system justification has been demonstrated in experiments that primed participants with criticisms of their social systems, including economic and political systems (e.g., Kay, Jost, & Young, 2005; Lavitan & Jost, 2014), justice systems (e.g., van der Toorn et al., 2014), and societal deterioration in general (e.g., Jolley et al., 2018; Yeung et al., 2014). These studies, conducted in the contexts of the U.S., U.K., and Canada, showed that participants exposed to system threats exhibited stronger perceived legitimacy of the system, increased system relevance, stronger national identification, decreased ideological gaps in national attachment, greater endorsement of stereotypes, heightened real-world conspiracy theories, and reduced support for legislation challenging the status quo compared to those in praise or control groups.

System Inescapability/Stability

Perceived inescapability or stability of the system is another contextual factor influencing system justification. Individuals, particularly those with low social status, high subjective powerlessness, and low perceived social mobility, are more likely to justify the system. They are motivated to rationalize irrevocable or unchangeable decisions (Aronson, 1969) to enhance self-control and reduce cognitive dissonance between their position and social reality. In such cases, self-interest is minimal, and system justification overshadows ego and group justification. When the system is perceived as traditional and longstanding (Blanchar & Eidelman, 2013; Shockley, Rosen, & Rios, 2016), the motivation for justification can occur passively and unconsciously through social learning processes. Jost (2020a) pointed to the caste system in India and the capitalist systems in Europe and North America as examples. Challenging the status quo or socio-political arrangements necessitates facing existential terrors related to safety and security, epistemic threats of uncertainty and unpredictability, especially in protest movements, and relational risks that might harm one's social relationships and networks (Jost et al., 2017). This

process is least likely among those with a strong need for order and closure, as acquiescing to the status quo may be an easier strategy to resolve cognitive dilemmas (Caricati & Owuamalam, 2020).

System justification is also stronger when a social situation becomes fixed and ongoing, such as when a new law is enacted and enforced. Compared to the pre-decision stage, in the pre-implementation and post-implementation stages of a new law, individuals are more motivated to justify and feel less annoyed by the new arrangement as they perceive changes as inevitable (Friesen et al., 2019). For instance, an experiment showed that participants exhibited more positive attitudes towards a government decision to lower speed limits in urban areas once the decision was made (Laurin et al., 2012). Similarly, during the U.S. elections in 2000 and 2016, respondents rated presidential candidates more favorably after they were elected compared to before the election and Presidential Inauguration.

System Dependence

Alongside perceived threats and system inescapability, outcome dependence is an independent contributor to perceived legitimacy, thereby reinforcing system-justifying biases (van der Toorn, Tyler, & Jost, 2011). Prior studies indicated that increased dependence on a system led participants to view the government as more responsible and benevolent (Kay et al., 2008), and policies related to the status quo as more reasonable and desirable compared to those not related to the status quo (Kay et al., 2009). System dependence relates to legitimacy, power, and a sense of control. Fiske and Berdahl (2007) defined power holders as those with legitimacy and control over resources affecting others's well-being. Conversely, van der Toorn et al. (2011) conceptualized outcome dependence from the perspective of the powerless, whose mental and physical health, safety, and economic well-being rely on authority control. Power, in its essence, "resides implicitly in the other's dependence" (Emerson, 1962, p. 32).

In a series of five studies conducted in both real-world and laboratory settings, van der Toorn et al. (2011) demonstrated that individuals dependent on academic authorities, police,

state government, or experiment evaluators exhibited higher tendencies towards legitimacy appraisals through increased trust and confidence in authority, empowerment of authority, and deference to authority. Outcome dependence not only led to high perceived legitimacy of power holders but also subsequently influenced voluntary deference and increased satisfaction with outcomes and contentment with one's situation.

Dispositional Drivers of System Justification

Low Social Status and Powerlessness

Both advantaged and disadvantaged groups tend to justify the system, but those in disadvantaged positions have a stronger motivation to do so. Individuals with low social status, low self-control, and feelings of powerlessness experience greater cognitive dissonance and dependence on the system. Empirical studies have demonstrated that feelings of powerlessness increase the tendency to legitimize racial disparities in criminal sentencing, the unequal distribution of wealth in society, and the gender wage gap (van der Toorn et al., 2015). Additionally, powerlessness fosters stereotypes towards the in-group and favorability towards out-groups perceived to have positive traits such as legitimacy, intelligence, and responsibility (Haines & Jost, 2000). Social status refers to one's position on the socio-economic ladder, while a sense of power indicates one's relative control over resources (Jost, 2020b). Individuals who feel powerless tend to rely on others for access to valued resources, rewards, and to avoid punishment. The internalization and rationalization process results in system endorsement, status quo justification, and submission to authority, even in the absence of procedural fairness and a demand for obedience. System justification is a goal-directed behavior, and the ultimate aim for disadvantaged groups is to satisfy epistemic, existential, and relational needs as outlined in SJT.

Need for Closure and Structure

A cognitive characteristic closely linked to satisfying epistemic needs by reducing uncertainty and ambiguity is the need for closure. Some individuals have a greater desire for "an

answer on a given topic, any answer… compared to confusion and ambiguity" (Kruglanski, 1990, p. 337). Webster and Kruglanski (1994) describe need for closure as encompassing five distinct aspects: preference for order, preference for predictability, decisiveness, discomfort with ambiguity, and closed-mindedness. These traits are also found in authoritarian personalities, which exhibit a higher tendency towards system-justifying bias. Such individuals prefer stability, tradition, and order as these offer an "easy way out" (Kelemen et al., 2014) for their information processing and cognitive needs. Studies across different countries, from capitalist democracies (Jost & Kay, 2010) to post-socialist contexts (Kelemen et al., 2014; Jost & Kende, 2020), have consistently shown that a need for closure correlates positively with authoritarian beliefs and conservative ideology, and negatively with the need for cognition. People who are less inclined to engage in deep thinking tend to quickly seek and rationalize available answers from the status quo.

Political Allegiance and Alienation

Individuals who are politically allegiant perceive themselves as integral parts of the political system and tend to "evaluate the regime positively, see it as morally worthy, and believe it has a legitimate claim to their loyalty" (Citrin et al., 1975). Political allegiance is not unique to disadvantaged groups; power holders also rely on the sources of their power and strive to protect the system that favors them.

Conversely, political alienation refers to individuals who feel estranged from existing social institutions, values, and leaders (Citrin et al., 2015). A negative association between system justification and political alienation has been found in post-communist societies such as Poland (Radkiewicz, 2007), Hungary (Hunyady, 2009), and the Czech Republic (Macek & Markova, 2004). Although politically alienated individuals and those with system justification tendencies share a sense of powerlessness, politically alienated individuals often isolate themselves from power and current socio-political norms. As they do not feel dependent on the system, they are not motivated to justify it. Furthermore, due to their political disorientation, they

are less likely to perceive the system as legitimate compared to those with high system justification motivation.

System Justification in Political and Authoritarian Context

While SJT applies to various life domains such as social, economic, gender, and political contexts (Jost, 2019), this study specifically examines its application within the political domain. The tendency to justify the system is a consequence of the interplay between personality variables, threat, socio-economic status, and preference for conservative or right-wing ideologies (Azevedo et al., 2017; Jost et al., 2003, 2007). Empirical studies consistently show that system justification is closely linked to political conservatism (Jost & Hunyady, 2005; Jost et al., 2003), right-wing partisanship (Kelemen et al., 2014; Osborne & Sibley, 2014; Vargas Salfate et al., 2018), social dominance orientation (Jylhä & Akrami, 2015), nationalism, and patriotism (Carter et al., 2011). Political conservatives tend to score higher on measures of system justification (e.g., Jost, Nosek, & Gosling, 2008) and exhibit tendencies towards system justification through climate change denial (Feygina, Jost, & Goldsmith, 2010), climate science distrust (Azevedo & Jost, 2021), and advantaged-group favoritism (Jost et al., 2003; Jost et al., 2004).

Previous studies indicate that nationalism (Wang, 2008) and political system support (Wang & Kobayashi, 2021) often result from exposure to state-led propaganda in the media. Wang and Kobayashi (2021) found that these effects are amplified when national system justification is triggered by national threats and outcome dependence. They argue that system justification occurs not only through psychological mechanisms but also through media communication. Similarly, feelings of powerlessness have been shown to increase the legitimation of authority, thereby fostering system justification (Jost, 2020b; van der Toorn et al., 2015). In another study, perceived high threats to the system heightened emotional and cognitive responses, leading individuals to retaliate against whistleblowers (Sumanth et al., 2011).

Stereotypes serve ideological functions (Jost & Banaji, 1994) or defence mechanism (Freud, 1946), by which the ideas of the dominant become the ideas of the dominated (e.g.,

MacKinnon, 1989), and legitimizing myths are used to justify the oppression of some groups by others (e.g., Sidanius & Pratto, 1993). Jost and Banaji (1994) argue that political systems that pursue to preserve the status quo at all costs may produce individuals whose minds work to preserve the status quo at all costs, as they operate within unequal social systems requiring substantial ideological justification.

Individuals with an "authoritarian personality" exhibit a stronger tendency towards system justification due to traits such as conventionalism, conformity, cynicism, moral absolutism, intolerance, and prejudice (Jost et al., 2003), as well as a desire to reduce insecurity (Adorno et al., 1950), especially under conditions of threat and need for closure (Webster & Kruglanski, 1994). Conservative beliefs and authoritarianism share a cognitive style that supports stability, clarity, and order (Jost et al., 2003), similar to right-wing ideology, which upholds structure, certainty, simplicity, and tradition (Jost et al., 2009). Status quo maintenance and resistance to social change are foundational to SJT. These findings have been confirmed in various countries, including the United States, Lebanon, Argentina, Sweden, Italy, Poland, Turkey (Jost et al., 2017), Hungary (Lönnqvist, Szabó, & Kelemen, 2021), and China (Li et al., 2020; Wang & Kobayashi, 2021).

Legitimation and Justification Through The Lens of System Justification

Although the SJT is built from the psychological perspective of disadvantaged groups who tend to justify the status quo, the theory also mentions several means to justify the system. These means include direct endorsement of certain ideologies, the legitimation of institutions and authorities, denial or minimization of system problems or shortcomings, complementary stereotyping, and rationalization. This study argues that these means should be further advanced to imply at least two points.

First, these means apply to both disadvantaged groups, who justify the unjust world they live in, and advantaged groups, who strengthen the current social order to maintain their power. Just like legitimation, justification is not only a spectacle for the masses but also a private theatre

for rulers, where they see their identity portrayed, confirmed, and justified (Barker, 2009). Therefore, both concepts need to be addressed from both sides, between those with power and those without. Second, although legitimation and justification are two distinct concepts, a normative relationship between them should be drawn. van Dijk (1998) argues that the speaker must represent an authoritative institution, linking such legitimation to institutional justification. In other words, justification focuses on the normative content or substance of (de)legitimation (Bexell et al., 2022).

Legitimation is more often used in SJT with the perspective of disadvantaged groups, described as having low social status, powerlessness, and dependence on the system. They tend to legitimize social, racial, gender, and economic inequalities to reduce cognitive dissonance and boost the palliative effect. Extant SJT-related literature finds legitimation associated with social hierarchy (e.g., van der Toorn et al., 2015), gender performance (Froschauer, 2016), socio-economic inequalities (e.g., Brandt, 2013; Caricati, 2016; Samson, 2018), and perceptions of social mobility (e.g., Day & Fiske, 2017).

System legitimation tendency is even stronger under threat conditions. In threat-salient situations such as terrorism, climate change, economic downturns, and natural disasters, people need to shore up perceptions (Friesen et al., 2019) and restore the system's legitimacy to reduce uncertainty, ambiguity, and insecurity. The effect of threats on increasing system justification motivation was found in experiments that primed participants with criticism of their social systems, including economic and political systems (e.g., Kay, Jost, & Young, 2005; Lavitan & Jost, 2014), justice systems (e.g., van der Toorn et al., 2014), and societal deterioration in general (e.g., Yeung, Kay, & Peach, 2014; Jolley et al., 2018) in the U.S., U.K., and Canada. Participants exposed to system threats, compared to those in praise condition or control groups, showed stronger perceived legitimacy of the system, increased system relevance, stronger national identification, decreased ideological gaps in national attachment, stronger endorsement of stereotypes, increased real-world conspiracy theories, and decreased support for legislation challenging the status quo.

When the system is perceived as traditional and longstanding (Blanchar & Eidelman, 2013; Shockley, Rosen, & Rios, 2016), the justification motivation operates at a passive and non-conscious level through social learning processes. People, especially those with low social status, high subjective powerlessness, and low perceived social mobility, are more likely to justify the system. System justification is also stronger when a social situation becomes fixed and ongoing, such as when a new law is promulgated and enforced. Compared to the pre-decision stage, in the pre-implementation and post-implementation stages of a new law, people are more strongly motivated to justify and feel less annoyed with the new arrangement as they perceive changes as inevitable (Friesen et al., 2019). For example, in an experiment, participants showed more positive attitudes towards the government's decision to lower speed limits in urban areas once the decision was made (Laurin et al., 2012). Additionally, studies show that in the U.S. elections of 2000 and 2016, respondents rated presidential candidates more favorably after they were elected.

Together with perceived threats and system inescapability, outcome dependence is an independent contributor to perceived legitimacy (van der Toorn et al., 2011), thus contributing to system-justifying bias. Prior studies showed that increased dependence on a system led participants to believe that the government is more responsible and benevolent (Kay et al., 2008) and policies related to the status quo as more reasonable and desirable compared to those not related to the status quo (Kay et al., 2009).

There is a need to address legitimation from both sides, between those with power and those without. For example, the conceptualization of system dependence relates to system legitimacy, power, and sense of control. From the perspective of power holders, these factors are seen as legitimacy and control over resources that affect others's well-being (Fiske & Berdahl, 2007). However, from the perspective of the powerless, these are people coerced and dependent on those resources. van der Toorn et al. (2011) conceptualized outcome dependence from the perspective of the powerless, whose mental and physical health, safety, and economic well-being

depend on authority control. Power, in its nature, "resides implicitly in the other's dependence" (Emerson, 1962, p. 32).

While legitimation in SJT studies is seen through the lens of the powerless, legitimization in political discourse involves the pursuit of power or the ability to interpret events and reality and have this interpretation accepted by others (Diamond, 1996). Legitimation and its antonym, delegitimization, both refer to the exercise of power concerning role and social identity concepts through discursive and argumentative strategies to justify and protect one's interests (Cap, 2008). The process of legitimizing or delegitimizing something, from the discursive perspective, involves recontextualization (Al-Tahmazi, 2015). It includes "actual wordings, explicitly expressed meanings, or something only implicit or implied in the original text or genre" (Linell, 1998) based on either political actors's ideological preferences (e.g., van Leeuwen, 2007) or social categorization such as in-group and out-group identity (e.g., Chovanec, 2010; Sowińska & Dubrovskaya, 2012).

4.2. The Present Study

Legitimation Strategies of the Party-state Over Years

Vietnam and the VCP have employed various legitimation strategies to maintain authority and legitimacy over the years. Before 1975, when the country was reunified under VCP leadership, the Party primarily relied on nationalism, socialist ideals, Ho Chi Minh's charismatic authority, and external recognition as its main sources of legitimacy (Le, 2012). Following a legitimacy crisis in the decade after reunification, marked by stagnant socio-economic conditions and a controversial military intervention in Cambodia, the VCP adopted the Doi Moi policy (Renovation) in the mid-1980s. This policy aimed to renovate the economic structure and open the country to foreign partners (Vu, 2994), marking an important transition from a "hard authoritarian" to a "soft authoritarian" state (Thayer, 2010), and shifting its legitimacy strategy from purely idealistic to a more rational, performance-based legitimation mode (Le, 2012).

Since the 2000s, facing the diminishing viability of state socialism and Marxism-Leninism, Vietnam's one-party state has attempted to steer the system towards a more democratic direction, emphasizing political freedom, human rights, rule of law, and constitutionalism (Thayer, 2009), along with social welfare policies to enhance social equality. This period also saw the adoption of a more rationality-based legitimation strategy. Research measuring legitimacy in various authoritarian regimes found Vietnam to be the only country in the closed authoritarian group employing more rational-legal legitimacy claims, a strategy typically used by electoral authoritarian regimes (Kyzym, 2021). A survey examining attitudes towards government institutions and political systems found that Vietnamese respondents exhibited higher levels of satisfaction compared to those in other authoritarian regimes (Nathan, 2020).

It is evident from previous studies that closed authoritarian regimes predominantly rely on identity-based legitimation strategies, such as references to the regime's ideology, foundational myths, or the person of the ruler, in constructing their legitimation mix (von Soest & Grauvogel, 2017). Performance-based legitimation strategies, however, seem particularly important for all authoritarian regimes.

Over the years, nationalism has been an indispensable discursive tool used to legitimize the VCP's monopolistic rule and the socialist state in Vietnam (Mai, 2019), similar to its role in legitimizing the communist regime in the post-Soviet context (Dukalskis & Gerschewski, 2020), and more recently, to justify the adoption of the bamboo diplomacy in foreign policy (Trinh & Vu, 2023). The VCP's performance-based, nationalism-based, and defensive legitimation strategies are most pronounced in maintaining a delicate balance between the U.S. and China rivalry (Dung & Ho, 2022). Alongside nationalism, political stability and Party unity are often presented as guarantors to justify government control over media and public discourse, and to eliminate dissent and political mobilization.

Theoretical Rationale

While justification and legitimation of controversial policies can be explained through various theories, SJT offers unique insights that make it particularly well-suited for this study. SJT provides a framework for understanding how cybersecurity narratives are constructed and how cybersecurity measures are enforced, especially within the Vietnamese context. Although SJT has predominantly been applied in psychological studies with a bottom-up approach (focusing on individual attitudes and beliefs), the theory's core tenets can also be examined from a top-down perspective, where dominant institutions actively manufacture system-justifying beliefs to shape public opinion.

First, the SJT intersects with terror management and securitization theory that often used in security studies to explain how existential threats and and mortality salience (Ullrich & Cohrs, 2007) are used to justify and securitize rigid measures. A central mechanism of SJT is that it meets people's epistemic, existential, and relational needs, creating a sense of certainty, security, and social belonging (Hennes et al., 2012; Jost & Hunyady, 2005). These needs become particularly relevant in the domain of cybersecurity, where individuals may perceive cyber threats as existential dangers. SJT's overlap with securitization theory thus reinforces the notion that people are more inclined to support restrictive policies if they perceive fundamental threats to their security. In the context of the VCSL, the government frames cybersecurity measures as essential defenses, catering to the population's need for safety amidst perceived foreign threats. This framing justifies the enforcement of restrictive measures, promoting public acceptance as a necessary safeguard.

SJT's concept of injunctification, where people treat descriptive norms as injunctive norms when how things are becomes how things ought to be, is essential in understanding the creation of cybersecurity norms. Injunctification leads individuals to defend the status quo, perceiving it as both prevalent and desirable. Past studies have shown that injunctification motivates people to criticize those whose choices diverge from these norms (Friesen et al.,

2019). This process is reflected in cybersecurity, where hypothetical cyber threats become normalized as reasons for law enforcement, creating the impression that strict cybersecurity practices are universally implemented and thus necessary. The VCSL narratives foster this injunctive effect, using hypothetical scenarios blurring the distinction between "is" and "ought" to present cybersecurity measures as actions that "everyone else is doing it so should you" and thus promoting their acceptance as essential and reasonable (Leeuwen, 2008).

Third, the power of status quo maintanance in SJT and the manipulation of uncertainty in threat politics of security discourse are closely linked. In the context with contentious politics or social movements, from the perspective of the power holders, manipulation of threats or uncertainty as a part of the securitization process is a critical driver that is used to achieve strategic goals including restriction of adversary's scope for action to make the other uncertain about one's actions while increasing one's certainty about the other's actions (Hassib & Shires, 2021). From the perspective of the mass, certainty about the outcomes such as social order and stability satisfy people's needs for consistency, coherence, and certainty (Jost et al., 2004) to reduce subjective uncertainty that subsequently resulted in not only tolerance of socio-political arrangement (van den Bos, 2009) and motivation of system justification tendency but also mitigate collective action (Osborne et al., 2019) and opposition. This is also another fundamental of the SJT, in which, people find the devil they know less threatening and more legitimate than the devil they do not know (Blasi & Jost, 2012) and certainty about the unknown (or know unknowns) (Cavelty, 2013) is more tolerable than uncertainty about the known.

Forth, authoritarianism and system justification are closely constructed (Wilson & Sibley, 2013) in the intersection of resistance to change, status quo maintenance, commitment on religion, traditonal, moral values (Lönnqvist et al., 2021), and worldview-supportive experiences (van den Bos, 2009). In addition, people with authoritarian personality are more likely to possess system-justification ideologies through social learning or experience with authority (Altemeyer, 1996) and socialization due to the strong tendency of unquestioning obedience and respect of

authority (Lönnqvist et al., 2021). The application of the SJT into the study increases the theoretical relevance of findings.

Fifth, the intergration of SJT is helpful to comprehend how the power constructs compelling narratives to resonate with public needs and achieve the manufactured consent (Jost, 2020). The study not aims to examine cognitive and psychological mechanism for system justification prevailed in media discourse but to investigate context, framing and priming strategies that the party-state used to trigger and prevail motivation of system-justification biases and beliefs among populace. For example, the study not looks for evidences of cognitive dissonance in media discourse but examines clues that may trigger the dissonance such as a portrayal of powerless internet users against the threatening and cascading consequences of cyber attacks that may lead to public support and legitimization of cybersecurity regulations. In other words, through the lenses of system justification mechanism, the study examines how the dominant groups construct and assert beliefs to captures citizens' psychological needs for security, coherence, and belonging make them more receptive to system-supporting measures as well as increasing legitimacy and authority of the government.

Given the controversial nature of the VCSL, its promulgation and enforcement require strong justification to gain public consensus and legitimacy. SJT's tenets reveal how the government may accommodate and neutralize resistance by addressing potential counter-narratives. By portraying cybersecurity as essential for national protection, the government manages to reduce public opposition, framing resistance as dangerous and oppositional to national interests. SJT therefore enables this study to analyze how system-justifying narratives accommodate and suppress social resistance, supporting an authoritarian regime's agenda in contentious areas like cybersecurity.

As Blasi & Jost (2006) argued, SJT has significant implications for law and advocacy, particularly in understanding the resistance that typically accompanies public policy initiatives and controversial legislation. SJT provides a valuable lens for analyzing the justification

strategies that authoritarian governments employ, making it particularly relevant to the study of the VCSL. Through SJT, this study examines how narratives crafted by the government appeal to citizens' fundamental psychological needs for stability, security, and social coherence, increasing system legitimacy and suppressing opposition. Consequently, SJT offers not only a comprehensive theoretical rationale for understanding cybersecurity discourse but also enhances our grasp of how dominant groups sustain power by constructing system-justifying beliefs.

While previous studies on legitimation strategies in Vietnam mainly focus on the regime and the VCP, this study examines the legitimation process of the VCSL through a comprehensive analysis of state-sponsored media discourse. The integration of SJT into this research aims to demonstrate the applicability of cybersecurity discourse within SJT's institutional approach, addressing the theory's lack of institutional focus.

SJT has traditionally been examined from a bottom-up perspective, especially among disadvantaged groups, focusing on individual psychological characteristics, beliefs, trust, and stereotypes to understand the justification process (e.g., Jost & Hunyady, 2005). However, there is a need for insights on institutional contributors to justification, specifically how advocates deploy narratives to amplify or dampen system-justifying motives and motivated social cognition (e.g., see Jost & Hamilton, 2005) of those whom they would persuade (Blasi & Jost, 2012), and to understand which institutions might benefit from being bolstered, and which should be challenged and changed (Friesen et al., 2019). Legitimation, especially in an authoritarian context, is not just about the ruling power delivering an ideology accepted by the people but also represents the society's sense to justify its power (Jost & Hamilton, 2005). SJT sheds light on this kind of representation, indicating latent social cognition represented in mass media discourse.

Legitimation from a top-down direction is similar to traditional legitimation approaches, focusing on how institutions and authorities justify their power and authority to the people. However, legitimation from SJT's top-down approach differs as it is not only achieved through

explicit strategies like promoting democracy, emphasizing economic growth, or appealing to historical legitimacy but also by influencing people's cognitive motivation and psychological mechanisms through fear, existential threats, and subsequently justifying political arrangements and defending the existing system, even if it leads to inequalities or injustices.

In understanding cybersecurity discourse through an institutional lens, it's essential to delve into various dimensions that shape the narratives, policies, and responses surrounding digital security threats. One significant aspect of the SJT is the persuasive power of framing, as elucidated by Blasi & Jost (2012). Framing refers to the strategic presentation of information to influence perceptions, attitudes, and behaviors. In the realm of cybersecurity, framing plays a crucial role in shaping how individuals, organizations, and governgments perceive threats and solutions. Advocacy strategies that fail to account for system-justifying motives, as highlighted by Blasi & Jost (2012), may prove ineffective or even counterproductive. Therefore, understanding the underlying motives and power dynamics within institutions is paramount for crafting persuasive narratives that resonate with diverse stakeholders.

A fundamental aspect of the institutional approach is recognizing the role of language in framing cybersecurity discourse. Cavelty (2013) emphasizes that understanding the language used to discuss the digital realm is essential, as it serves as the foundation for constructing cybersecurity narratives. Terms such as "cyber threats" and "digital infrastructure" carry implicit meanings that shape perceptions and attitudes toward cybersecurity issues. Therefore, fluency in this language is a crucial first step in analyzing cybersecurity discourse within institutional contexts.

Moreover, the news media play a significant role in shaping societal understandings of cybersecurity threats. Boholm (2021) argues that media representations reflect and reinforce prevailing narratives about social problems, including cybersecurity threats. By analyzing news coverage, researchers can gain insights into how these threats are framed and understood in

society, shedding light on the influence of media in shaping public perceptions and attitudes toward cybersecurity issues.

The genealogy of cybersecurity discourse reveals the influence of institutional structures and interests in shaping threat narratives. Cavelty (2017) highlights how material conditions, such as geopolitical tensions and technological advancements, determine the perceived risks and vulnerabilities in the digital realm. Understanding the interests and agendas of institutional actors is crucial for unraveling the underlying power dynamics that shape cybersecurity discourse.

Political regimes also play a significant role in shaping cybersecurity discourse, particularly in terms of system justification motives. Babb (2022) suggests that authoritarian regimes, reliant on performance-based legitimacy, are particularly vulnerable to factors undermining their ability to meet societal needs. By prioritizing control and suppressing dissent, these regimes may influence the framing of cybersecurity threats to maintain their authority. Understanding the political context is essential for grasping the motivations and strategies of institutional actors within such regimes.

Moreover, ideological factors influence the legitimization of power structures and governance practices, as emphasized by Kneuer (2017). Ideologies prescribe worldviews and provide instructions for shaping society, serving as a justification for authoritarian rule. Analyzing the ideological dimensions of cybersecurity discourse provides insights into how regimes seek to legitimize their authority over digital spaces.

In short, an institutional approach to system justification should focus on manifest factors existing in policies, procedures, practices, traditions, documents, and physical spaces of institutions (Jost, Federico, & Napier, 2009). A study of media discourse on cybersecurity helps reveal the persuasive power of "framing" (Blasi & Jost, 2012), the language used to discuss the digital realm (Dunn Cavelty, 2013), and understandings of socio-technological problems (Boholm, 2021). It also shows how possibilities and impossibilities of threats and countermeasures determine the shape of danger discourse (Deibert et al. 2008). Studying system

justification from a top-down approach requires identifying key speakers and underlying power relations, their communicative strategies, evaluating impacts, and contextualizing justification claims (Abulof & Kornprobst, 2017). As security culture reflects societal behaviors, attitudes, and values (Górka, 2023), the top-down approach helps examine how authority frames and exploits these values to resonate with audience motives.

Research Objectives

This study is theoretically built on the SJT, which posits that individuals are motivated to defend, justify, and bolster the status quo and political arrangements, particularly when the system is perceived as inescapable, longstanding, or under threat. The tendency towards system justification is likely to be stronger among those who perceive themselves as powerless, have a need for closure and structure, and are dependent on the political system and fear alienation. Justification can thus be achieved through the direct endorsement of certain ideologies, the legitimation of institutions and authorities, denial or minimization of system problems or shortcomings, complementary stereotyping, and rationalization. The construction and perpetuation of specific narratives and ideologies are crucial to authoritarian nations, especially single-party regimes (Babb, 2022). Although these postulates are made from the perspective of disadvantaged groups, this study seeks attributes and context of these processes in the political discourse or propaganda of power holders, in this case, Vietnam's party-state and its mouthpiece, state-sponsored media. In other words, the study examines how rulers use state-sponsored media to cultivate cognitive heuristics and align propaganda discourse with people's cognition to generate and facilitate their system justification motives.

The thesis consists of three studies.

Through an examination of media presentations on the VCSL, the first study seeks discursive and heuristic evidence of situational attributes for system justification motivation through the presentation of state-sponsored media on cybersecurity threats (existential threats) that endanger national security, network security, and the rights and interests of individuals and

organizations. In contrast to the bleak scenario threatening human existential needs, the study also examines how media discourse justifies and bolsters the VCSL through the projection of promising outcomes of the law (outcome dependence) and the importance of social order and stability (status quo). To demonstrate the subjectivity and bias toward law justification in state-sponsored media, the study undertakes a comparative analysis of the discourses on cybersecurity and the VCSL as presented by national and international media outlets. The primary goal of this comparative analysis is twofold: to investigate how cybersecurity is framed, which cybersecurity topics are chosen to be covered, and how the VCSL is positioned differently through language usage in national and international media discourses. Additionally, the study captures the dynamic and reflexive nature of the linguistic constructions adopted by the two media actors, thus facilitating further investigation into the diversity and opposition inherent in their framing strategies.

If the first study examines contextual factors, the second study looks for evidence of dispositional attributes, analyzing factors that trigger cognitive motives for system justification through the positioning of powerless lay people in contrast to the powerful party-state and assigning rights and obligations to relevant stakeholders. Specifically, the study analyzes how state-sponsored media emphasize the powerlessness of laypeople amidst cyber threats and an inescapable shared reality (sense of powerlessness) to strengthen the need to rely on the great leadership of the party-state (political allegiance). More importantly, through state media discourse, the party-state also triggers one of the most prominent authoritative characteristics, the need for closure or orientation, by assigning rights and obligations to individuals, organizations, state leaders, and involved parties under the enforcement scope of the VCSL.

The final study analyzes media discourse from a different angle, examining system justification strategies that the state and mainstream media use to legitimize the cybersecurity law in general and controversial regulations specifically. This study focuses on five ideological strategies guided by SJT: authorization, rationalization, moralization, denial of system problems, and stereotyping or the delegitimation of these elements. Only through a comprehensive

examination of text and its context can the study reveal latent ideologies and justification strategies in the rationalization process of state and media actors.

Main direction for analysis is summarized in Table 1.

Situational factors	Epistemic, existential, and relational needs	Cybersecurity threats on national security and individuals
	System stability (Status quo)	Status quo in Vietnam and legitimacy of power holders
	Outcome dependence	Projected outcomes of cybersecurity law implementation
Dispositional factors (The positioning of us vs them and the government's stance)	Sense of powerlessness among disadvantaged groups	Positioning of "powerless" lay people amidst cyber attacks and hostile acts
	Need for closure and orientation	Rights and obligations of the powerful and the powerless
	Political allegiance and alienation	Party-state's discourse on patriotism, nationalism, and alienation of hostile forces
Justification strategies	Authorization	Impersonal authority Personal authority Authority of conformity
	Rationalization	National security Information security Rights and interests of individuals and organizations Social order and stability Need of legal corridor development Economic development
	Moralization	Legitimation of moral values Legitimation of cultural standards/customs
	Denial of system problem	Power abuse Control of personal data Violation of freedom of expression Creation of business barriers

		Violation of international agreements
	Stereotyping/delegitimation	Hostiles and reactionary forces Foreign media/organizations

Table 1. Summary of Main Analyses in Study 1, Study 2, and Study 3

Chapter 5. Media Presentations of Vietnam's Cybersecurity Law: A Comparative Approach With Corpus-Based Critical Discourse Analysis*

**This study was published on Computer Law & Security Review in June 2023.*

Nguyen, M. QMN. (2023). Media presentations of Vietnam's cybersecurity law: A comparative approach with corpus-based critical discourse analysis. Computer Law and Security Review, 50, Article 105835. https://doi.org/10.1016/j.clsr.2023.105835

5.1. Research Objectives and Research Design

The first study in this thesis provides an overview of media presentations on cybersecurity and the VCSL. It explores the context, keywords, main topics, and social events highlighted in news articles relating to the promulgation and enforcement of the law. Importantly, it addresses securitization construction by identifying security grammars such as security actors, security topics, cyber threats and harmful behaviors, referent objects (or endangered values), referent subjects, and stakeholders. By comparing and contrasting national and international media discourses, the research seeks to illustrate how different angles and contextual factors contribute to the subjective construction of cybersecurity. While the nature of this study is descriptive, its ultimate objective is to provide evidence of situational factors, demonstrating how state actors use regime-controlled media to create a sense of existential threats among citizens and contextualize the need for cybersecurity in the country.

To achieve this objective, the study employs a mixed-method approach that includes keyword analysis, topic modeling, and corpus-based critical discourse analysis. Notably, the study undertakes a comparative approach to analyze discourses on cybersecurity and the VCSL as presented by state-sponsored and international media outlets. This means examining both primary securitization (state-sponsored media discourse) and counter-securitization (international media discourse). State-sponsored media serve the political leaders and decision-makers in achieving their securitization objectives, shaping the audience's perception in line with

government interests (Górka, 2023). In contrast, international media, being independent of state control, provides diverse viewpoints, global information resources, and counter-arguments for public debate.

The primary goal of the comparative analysis of the two discourses is twofold. First, the study aims to investigate how cybersecurity is framed, which cybersecurity topics are chosen for coverage, and how the VCSL is positioned differently through language usage in national and international media discourses. Second, as the existing literature lacks analysis of rival views (Baysal, 2020) on the same speech acts, the study captures the dynamic and reflexive nature of the linguistic constructions adopted by the two media actors, thus facilitating further investigation into the diversity and opposition inherent in their framing strategies.

5.2. Research Method and Materials

Corpus-based Critical Discourse Analysis

Corpus-based critical discourse analysis is a method that belongs to the corpus-based approaches, which are built on the construction of vocabulary lists (West, 1953), corpus linguistic features, and associative relationships between words (Gablasova, 2021). The approaches are mainly applied in two avenues of inquiry: either to tap into language production with an examination of corpus evidence or to compare association response patterns between speakers (Gablasova, 2021). In cybersecurity studies, particularly, the methodology is used in semiotic analysis of laws and legal terms, cybersecurity legislative discourse analysis (Cheng, 2019), and institutional discourse of critical information infrastructure protection (Cheng, 2021) with an emphasis on analyzing securitizing actors and referent objects. The method is also used in cybersecurity discourse analysis with comparative elements between genres (Rackevičienė et al., 2022), and between media organizations and countries to contrast discourse characteristics in language production (Pei et al., 2022).

Corpus-based critical discourse analysis is an integration between Corpus Linguistics (CL) and Critical Discourse Analysis (CDA). CL and CDA are different in many aspects.

Corpus linguistics is regarded as a methodology and an approach to language data rather than a theory (Flowerdew, 2012). It encompasses five categories of co-selection, including core lexical item, semantic prosody, collocation, colligation, and semantic preference (Sinclair, 2004). By studying a large collection of both spoken and written texts in the computerized database and corpora (Kübler & Zinsmeister, 2015), CL brings a quantitative dimension to language description by providing information on the probability with which linguistic items or processes occurring in particular contexts (Kennedy, 2001). CL analysis is based on the computation of frequencies and keyness of words to explore frequency lists, keywords, clusters, collocation, and concordance lines. This approach not only provides an overall description of the corpus and how the language is used in a particular context but also draws a broader picture of the immediate textual surroundings of a specific word (Pei et al., 2022). CL is useful for examining language variations systematically in different historical, regional, and sociolinguistic contexts, genres, and registers (Kennedy, 2001). In this study, CL helps quantify the differences in language usage surrounding the VCSL between state-sponsored and foreign media.

Greatly different from CL, CDA does not treat text as a quantitative product but emphasizes the integrity of text, socio-political and cultural context, and the construction of data to unravel discourse as a social process and social action. In other words, CDA examines the "connections between the use of language and the exercise of power" (Fairclough, 1995) to reveal the relationship between ideology and rights behind the language (Romaine, 2000). Especially in news analysis, CDA also uncovers misdirection and discrimination in various modes of public discourse as news reportage is not solely dependent on the event itself but on the lexical choices of reporters, interests of the individuals or groups they represent as well as how they target the audience psychologically (Zhang et al., 2022).

CDA comprises three dimensions, which are text, discursive practice, and social practice. However, to avoid an approach that focuses mainly on "lexicon-grammatical meaning in written and mass-mediated texts" (Blommaert, 2001), that it fell short in accounting for processes of production and reception (Philo, 2007), the study places greater attention on the other two levels, where discourse becomes discourse-as-ideology with the focus on the meanings, representations, or ideologies embedded in the text (Carpentier, 2017).

Although CL and CDA differ ontologically and epistemologically (Virtanen, 2009), the application of corpus-based critical discourse analysis aims to leverage the strengths of both approaches. By supplementing one another, the study seeks to describe media's presentations and uncover the cognitive, social and political factors that constructed discourses surrounding the VCSL.

Data Collection

The study builds two text corpora. The first corpus is the "State-sponsored News' or "National News," which consists of online news articles relating to cybersecurity issues and the VCSL from various sources. These sources include Vietnam's state-sponsored media outlets (i.e., official media organizations owned or operated by the party-state system), aggregated news websites (i.e., webpages run by business corporate and licensed by the Ministry of Information and Communication), and party-government organizations (e.g., Vietnam's Central Committee for Propaganda and Education, Ministry of Public Security, Ministry of Defense, Vietnam's Communist Party…). These organizations have their websites to deliver public information. The second corpus is the "International News," which contains news articles relating to Vietnam's cybersecurity issues and the VCSL from recognized foreign media outlets and international organizations that usually have a strong influence on international media, such as Human Rights Watch, Amnesty, Freedom House, Reporters Without Borders. The inclusion of news from these organizations is important since they are actively involved in commenting on and analyzing

cybersecurity issues in Vietnam. In addition, they are served as reference news sources for other media outlets.

Online news articles in both corpora were manually retrieved and collected using the search function on Google News and Yahoo News with seeding keywords in both Vietnamese and English such as “Vietnam cybersecurity,” “Vietnam cybersecurity law,” and “Vietnam information security.” The search started with generic terms aimed to avoid biases and partiality in the data. However, during the data collection process, once an article from a news outlet was obtained, the author continued to collect relevant or suggested articles from the outlet until no new content was found. In both corpora, articles that simply conveyed the content of the related law and its regulations were eliminated, as they did not provide any further argument or justification. Articles written in Vietnamese were translated into English for data analysis in the subsequent step.

The data collection for this study spanned from the end of 2017 to October 2022. It was in late 2017 that Vietnam’s media began systematically and extensively covering cybersecurity issues and the drafting of the VCSL. The year 2018 marked an important milestone as it yielded the highest number of news articles compared to other years in both corpora. This was due to the drafting, discussion, and eventual passage of the VCSL at Vietnam's 14th National Assembly, which came into effect in January 2019.

After the screening step, there are 425 news articles in the national corpus and 269 articles in the international corpus. The distribution of news by sources and years is shown in the charts below.

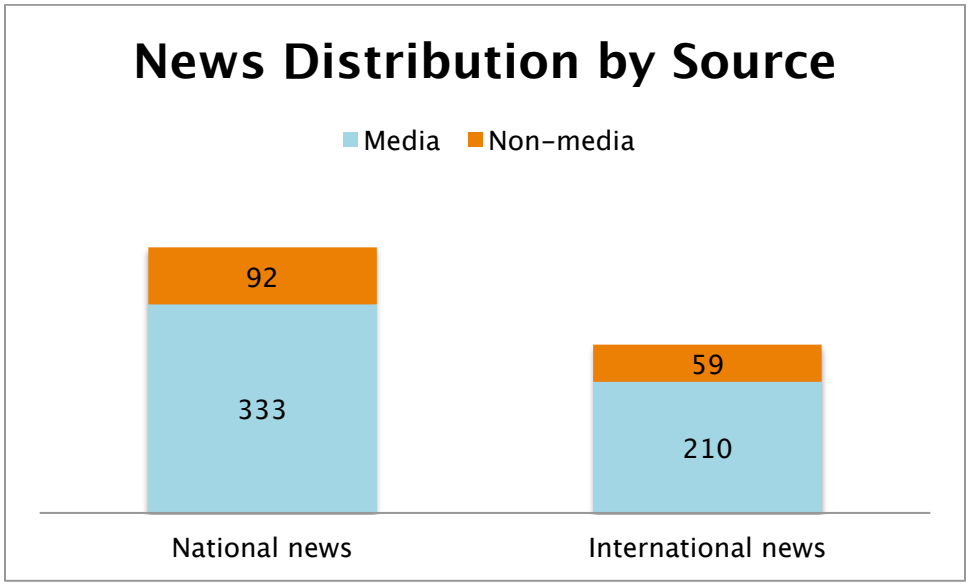

Chart 1. News Distribution by Sources

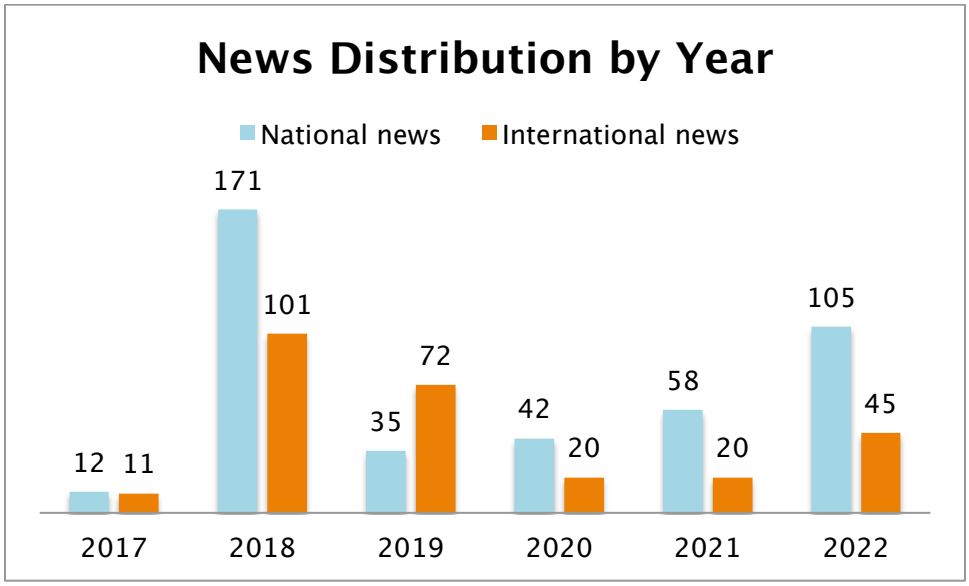

Chart 2. News Distribution by Year

Data Pre-processing

The data in the text corpora were first pre-processed by removing stopwords, punctuations, special characters, converting words to lowercase with Natural Language Toolkit NLTK package, and then, were tokenized for analysis. The national news corpus has 217,738 tokens with 6,972 unique words and 2,193 words that appeared only once. The international corpus contains 117,780 tokens with 6,964 unique words and 2,495 words that only appeared once.

Data Analysis

After the pre-processing step, the study used the Counter package from NLTK to extract single keywords for keywords comparison; webtext, nltk.collocations, and gutenberg package from NLTK to explore bigram and trigram collocation and concordance lines; and LDA (Latent Dirichlet Allocation) Mallet for topic modeling.

Single keyword exploration with NLTK involves extracting the most frequently occurring keywords to identify important words and phrases in the text corpus. Meanwhile, the exploration of collocation and concordance of keywords is based on calculating the log-likelihood ratio between the observed and expected frequencies of n-grams (bigrams and trigrams). The log-likelihood ratio helps determine the statistical significance of co-occurrences. Higher scores indicate more significant collocations. Although an analysis based on the log-likelihood ratio cannot be used to compare scores across corpora, it is useful to uncover preferences for framing the cybersecurity issues and the VCSL and understanding their textual surroundings in different types of media.

Finally, topic modeling technique is helpful to visualize content maps with different topics present in the corpus (Törnberg & Törnberg, 2016). In this study, unsupervised topic modeling LDA was used to discover topic and topic proportion based on Dirichlet distribution.

The study optimized the number of topics ranging from 5 to 30 to find the best model that captures the most inclusive content map of the news corpus.

The results showed that, in both corpora, the model with 8 topics provided the best fit, as the more topics in the model, the more they overlapped. To enhance the accuracy of labeling these topics, the study used the LDA Mallet model to examine dominant documents and keyword distribution within each topic. This allowed for capturing the most frequent context in which certain keywords appeared. The computational analyses conducted at this step provided descriptive features for the dataset and established the foundation for more comprehensive manual data analysis in the subsequent steps.

5.3. Findings

Keywords Comparison

The results from keyword identification based on frequency in the national news and international news corpora show some common keywords, such as *information, security, cybersecurity, rights, national, organizations, data*. Cybersecurity discourse in the national news corpus primarily revolves around security and information infrastructure (including terms like *information, security, cybersecurity, cyberspace, network, data, internet,* and *services,*) economic infrastructure (with words like *system, enterprises, foreign, businesses,* and *economic,*) legislative and institutional words (such as *law, national, Vietnam, social, state, agencies, organizations, ministry, acts,* and *assembly,*) human-centric words (involving words like *people, individuals, public, personal, users,* and *human,*) and securitizing referent objects (such as *rights, freedom, order, interests,* and *safety*). In addition, positive adjectives referring to the VCSL are present such as *important, legal, legitimate,* and *lawful*. Table 2 and Table 3 display the top 50 unique keywords from the national and international news corpora.

Rank	Word	Frequency	Rank	Word	Frequency

6	law	2420	56	agencies	341
8	security	1967	57	foreign	335
10	information	1679	58	protect	321
13	national	1355	59	freedom	319
14	cybersecurity	1322	61	enterprises	318
16	vietnam	1080	63	personal	304
19	cyberspace	834	66	businesses	295
21	people	761	67	users	293
24	network	701	68	acts	292
27	social	672	70	important	287
29	cyber	627	72	protection	284
31	rights	619	74	ministry	282
32	data	597	75	facebook	281
34	organizations	569	77	countries	280
36	state	544	78	legal	274
37	order	536	81	government	253
41	activities	478	82	economic	252
42	assembly	473	83	safety	251
43	internet	454	86	business	243
44	individuals	427	87	human	243
46	interests	402	89	article	242
50	public	358	91	content	233
53	country	345	92	provisions	233
54	services	345	93	legitimate	232
55	networks	344	94	systems	230

Table 2. Top 50 Unique Keywords by Frequency in the National News Corpus

The international news corpus, on the other hand, predominantly consists of content related to information infrastructure (such as *data, information, internet, media, online, content, cyber, digital, service, store,* and *technology*), legislative and institutional words (including *law, government, country, national, ministry, authorities, assembly, part, communist, bill,* and *draft,*) as well as words referring to the actors and stakeholders involved in the VCSL (such as *Facebook, Google, China, Asia, global, international*).

Rank	Word	Frequency	Rank	Word	Frequency
7	vietnam	1065	60	ministry	161
8	law	925	61	content	160
14	cybersecurity	459	65	state	147
14	government	444	68	international	137
16	data	443	69	cyber	136
22	vietnamese	355	70	freedom	134
24	facebook	347	72	economic	131
26	information	316	73	human	131
27	security	313	74	assembly	128
28	internet	298	75	local	128
30	new	296	78	june	120
32	people	280	80	digital	117
36	companies	271	81	user	115
38	media	263	83	party	112
40	country	253	85	communist	106
42	online	233	92	store	101
44	national	216	93	bill	100
47	rights	209	94	hanoi	100
49	foreign	200	96	global	97
50	google	196	97	asia	96

51	users	194	98	service	95
55	social	174	99	personal	93
56	public	169	101	protests	90
58	china	167	103	draft	88
59	authorities	165	104	technology	88

Table 3. Top 50 Unique Keywords by Frequency in the International News Corpus

Topics Comparison

National News Corpus. The results from LDA topic modeling reveal several main topics that shed light on different aspects of the VCSL. The largest topic (32.6%) in the corpus provides an overview of the law and encompasses the most frequent words like *cyberspace* and *cybersecurity*, and other generic words that indicate the state's legal corridor and information infrastructure including *security, network, law, system, legal, Internet, information*, as well as security activities such as *protection, development,* and *ensure*. The second largest topic (19.1%) emphasizes the mission of the party-state to *ensure* legitimate rights of *citizens*, *individuals, people,* and *public* including concepts like *freedom, information,* and *speech*, as well as to *prohibit* harmful acts that *violate* these rights.

The third (13.3%) and the sixth topic (9.5%) highlight cyber threats, which encompass harmful behaviors such as *spreading fake news*, *false information* that *violate social* norms or harm *individual* reputation on social media, and more dangerous *attacks* that are considered *cybercriminal* targeting *digital*, *business*, and *banking* system. While this topic refers to human-related threats, the sixth topic indicates technique-related threats such as *phishing* and *malware*. The forth (13%) and fifth (12.4%) topics bolster the benefits of the VCSL in improving the cyber environments, such as *safety* and *technology* for *digital transformation*, *business,* and *economic development*. The seventh topic includes words related to the 14th National Assembly, such as *delegates, agreed, fairness, feasibility,* and *ambassador*.

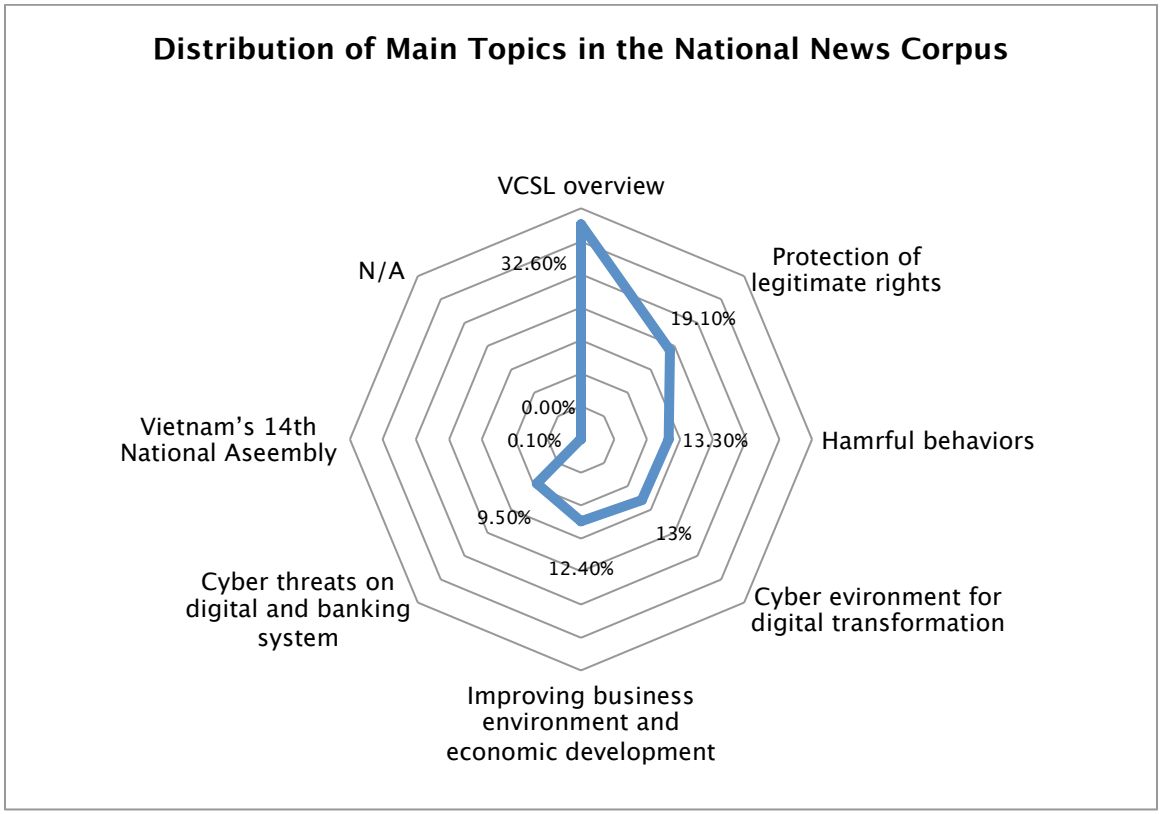

Chart 3. Distribution of Main Topics in the National News Corpus

International News Corpus. The international news corpus also reflects the two biggest debates on the VCSL regarding human rights and business issues, but from a different perspective. The largest topic (37%) reveals international concerns about human rights violations, involving actors such as *activists, authority, police, Facebook* and strong verbs like *arrest, force, charge, report,* and *protest*. The third topic (19.2%) addresses data localization regulation, which is also a significant international concern regarding business issues. The forth topic (17.1%) focuses on the removal of sensitive and illegal content on social media, targeting major platforms such as Facebook, Google, and YouTube. The remaining four topics, accounting for 5.1% of the whole corpus, cover ongoing social events, opposition, and criticism against the VCSL from different sources. The fifth topic covers demonstrations against the exclusive economic zone and cybersecurity law bills in June 2018, with keywords such as *protest,*

protester, *cybersecurity*, *police*, *special*, *zone*, *lease*, *demonstration*, *beat*, *land*, *arrest*, *bill*, *province*, *investor*, *street*, and *participate*. This topic is not present in the national news corpus. Other minor topics provide comments and criticism from journalists, experts, and Vietnamese intellectuals regarding the VCSL, with keywords such as *critic*, *dissent*, *absurd*, *debate*, and *scandal*.

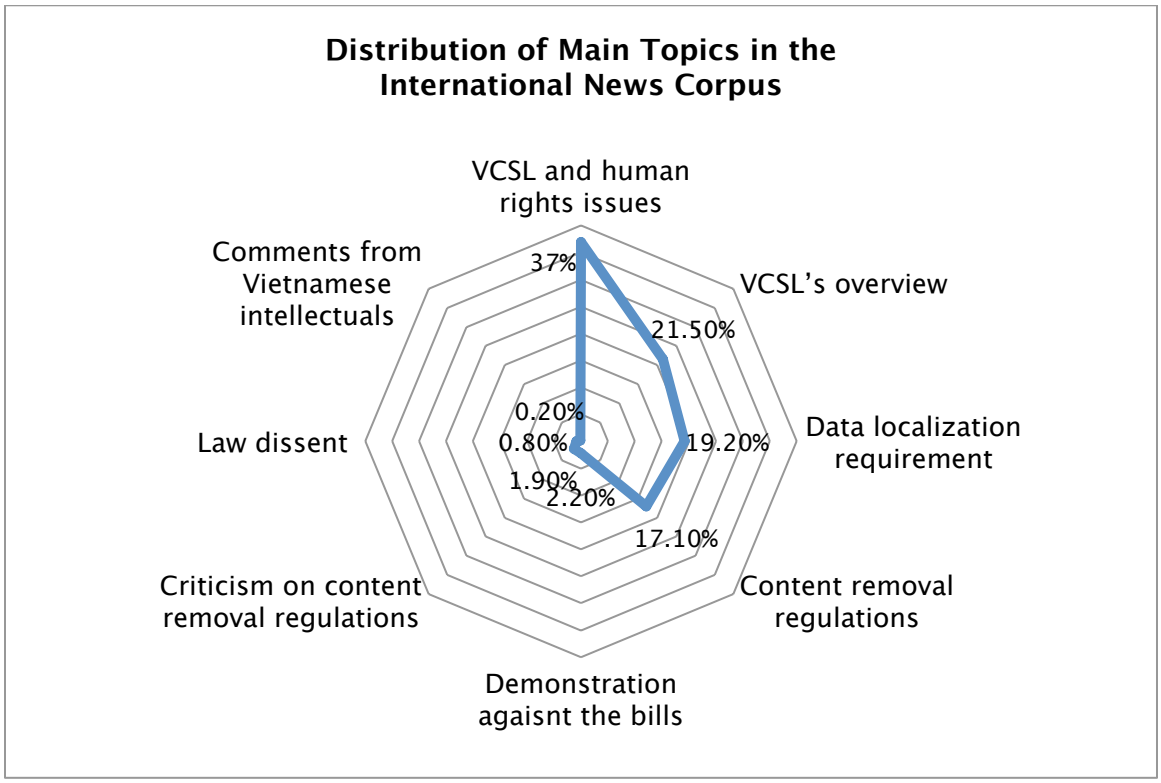

Chart 4. Distribution of Main Topics in the International News Corpus

Despite some fundamental differences, the two corpora share a common topic characterized by similar generic keywords, which contribute to an overarching understanding of the VCSL.

Security Elements Comparison

The identification of bigram and trigram collocation provides a basic but essential understanding of subjects, objects, endangered values, means, actors, and acts within the realm of cybersecurity discourse.

Overall, the national news corpus highlights the presence and seriousness of cyber threats, thereby reinforcing the underlying objectives of the VCSL. Noun phrases in the national news corpus reveal a media's emphasis on cybersecurity issues at both the national level (*national security, network security, social order, national defense, state secrets)* and the individual level (*personal information, human rights*, *legitimate rights*). Furthermore, cultural values and moral goodness, such as *fine customs, customs traditions,* and *revolutionary achievement,* are also acknowledged as endangered values.

The most frequent noun bigrams also signify cyber threats attributed to human-related actors, such as *hostile forces, reactionary forces, cyber espionage,* and *hi-tech crimes,* through *illegal acts* and *prohibited acts* such as *riot disrupt, deny revolutionary, spread false, history deny, humiliate slander, religion discrimination, discriminate gender*. In addition, technique-related threats like *malicious code, hackers, malware,* and *viruses* are also prevalent. Strong verb phrases are used to underline the danger associated with these acts such as, *infringing upon, taking advantage, causing trouble, inciting riots,* or *denying revolutionary achievements* .

In response to the presentations of cyber threats, the national media bolstered the mission of the state and government in safeguarding endangered values through *crime prevention* and enhancing *security protection, defense security*. Consequently, the VCSL serves as a *legal basis, a legal corridor* to *prohibit acts, handle violation, serve investigation*, and *raise awareness*. The law is also highlighted as momentum for *digital transformation* and the *industrial revolution*.

Elements	Key phrases
Engendered values	*National level*

	national networks, national security, network security, social order, order safety, national defense, state secrets, public security, unity bloc, network security, cybersecurity, information security, *Individual level* human rights, legitimate rights, freedom speech, freedom press, rights interests, private life, personal information, honor dignity, honor reputation *Cultural values/moral goodness* fine custom, custom tradition, revolutionary achievement
Cyber threats	*Human-related* hostile forces, hostile reactionary, cyber attacks, cyber espionage, fake news, false information, hi-tech crime *Technique-related* malicious code, hackers, malware, virus
Harmful behaviors	illegal acts, prohibited acts, illegal acts, cause damage, riot disrupt, deny revolutionary, spread false, history denial, humiliate (and) slander, religion discrimination, discriminate gender, cause confusion
Target actors/stakeholders	organizations (and) individuals, foreign enterprises, domestic foreign (companies), agency organizations, Facebook, Google, service providers, duty performers
Purpose of VCSL	digital transformation, crime prevention, raise awareness, handle violation, prohibit acts, security protection, defense security, legal corridor, serve investigation, legal basis, industrial revolution

Table 4. Annotation of Top Bigram Collocations in the National News Corpus

In contrast, the presentation of the VCSL in international news exhibited a more neutral discourse on the law's content by using generic, law-related nouns to refer to different stakeholders. These included terms such as *national assembly, communist party, service providers, Facebook Google, Amnesty International, chamber* (of) *Commerce,* and *foreign companies*. Neutral verbs such as *take effect, store data, remove content, and come effect* were commonly used. Two areas of common ground between the two corpora were the emphasis on

data localization, the requirement of setting up *representative offices*, and individual-related concerns in cybersecurity, including *human rights* and *freedom of speech*.

Elements	Key phrases
Cybersecurity and VCSL	public security, personal data, take effect, information communication, new law, social network, store data, representative offices, data localization, national security, user data, remove content, Penal code, digital economy, foreign investment, Google Facebook, information system, localization requirement
Human rights issues	human rights, freedom expression, free press, prisoner (of) conscience, rights groups, economic zone, devastating consequences, years (in) prison, potentially devastating, Mai Khoi, Nhu Quynh, Mother Mushroom, Doan Trang
Actors and stakeholders	national assembly, communist party, Vietnamese authority, Xuan Phuc, prime minister, general secretary, Vietnamese government, Facebook Google, Amnesty International, foreign companies, (human) rights watch, chamber (of) Commerce, technology companies
Censorship	censorship tolerance, severe limitation, tight medium, retain tight, illegal content, tolerate little, totalitarian model, deeply repressive

Table 5. Annotation of Top Bigram Collocations in the International News Corpus

5.4. Discussion

Media Framing on Cybersecurity and the VCSL

To provide a more nuanced analysis of the disparities between national and international discourse surrounding a common subject, a collocate comparison and concordance lines were conducted for the term *cybersecurity*. The main purpose of this analysis was to examine the divergent linguistic strategies employed by distinct media sources in framing discussions related to cybersecurity issues and the VCSL within the country.

Corpus	Collocation of "cybersecurity"		
	Nouns	Verbs	Adjectives
National news	law, protection, department, index, content, bill, field, information, safety, strategy, provision, implementation, information, expert	stipulate, pass, prohibit, consist, bear, promulgate, require, devote, charge	hightech, global, clearly, important, necessary
International news	law, bill, taskforce, incident, emergency, zone, protection, legislation, Vietnam, implementation, vulnerability, department, prevention	culminate, specialize, tighten, obstacle, propose, facilitate, improve, oppose, stipulate, audit, threat	new, controversial, contentious, draconian,

Table 6. Top 30 Collocates of the Word *Cybersecurity* in the Two Corpora

Bigram collocation analysis shows that when addressing *cybersecurity* and *cybersecurity law*, national media used either neutral or positive terms regarding law enactment and enforcement such as *protection, bill, information, implementation, provision, stipulate, pass, consist, promulgate, require, high-tech, global*, *important, necessary*. In addition, trigram collocation findings show that national media often use a combination of a positive adjective and noun to emphasize importance of the VCSL such as *important national security*, and *comprehensive cybersecurity law*. Furthermore, a combination of a verb and noun reveals the identifying clause between an action verb and its direct object noun, such as *National Assembly listened, protect national security, ensure network security* to show the transparent and proactive law promulgation. On the contrary, international media tend to use negative terms to indicate the law such as *obstacle, oppose, threat, controversial, contentious, draconian*, *human rights abuses,* and *human rights violations*.

Figure 1. Sample Concordance Lines of *Cybersecurity* in the National News Corpus

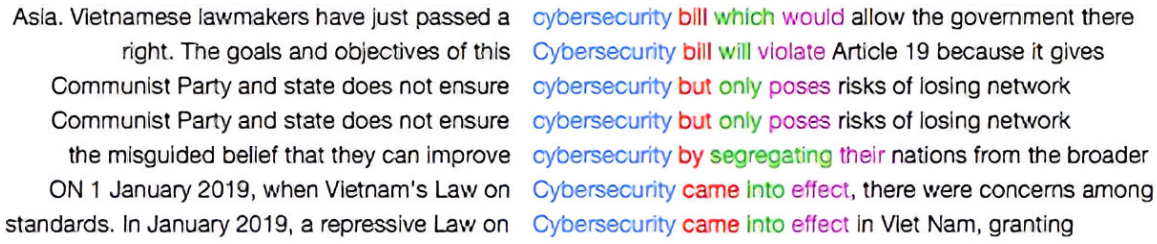

Figure 2. Sample Concordance Lines of *Cybersecurity* in the International News Corpus

State-sponsored Media: Cybersecurity as a Part of National Security. State-sponsored media discourse on cybersecurity and the VCSL, unsurprisingly, is a complexity that is primarily driven by political factors. This arises from the inherent connection between cybersecurity and political stability (Romaniuk & Manjikian, 2021) as well as the wide array of cyber threats that are perceived as potential threats to national security.(Mishra, 2020) Cybersecurity is not only conceptually constructed as safeguard goals (Fichtner, Pieters, & Teixeira, 2016) to cope with technical threats that destruct information networks but also, more importantly, to establish a legal surveillance system aimed at regulating harmful behaviors that pose risks to national security, national defense, unity bloc, and other long-standing values upheld by the regime.

According to state-sponsored media, the unity and stability of the state face significant risks due to the actions of reactionary forces who exploit democratic freedoms to engage in various activities. These activities include: 1) sabotaging ideology, sabotage internal affairs, carry out plots of *peaceful evolution,* cause national conflicts, incite protests and riots to

transform political institutions in Vietnam; 2) inciting illegal protest and gatherings to disrupt social order and security, incite violence, terrorism, regime overthrow, sovereignty and national unity infringement; 3) engaging in information misappropriation, revealing state secrets, revealing personal information; 4) sharing information that distorts state policies and party line, disrupting national unity, disgracing religions, disseminating disinformation, insulting and slandering organizations and individuals; 5) cultivating "poisonous mushrooms" that are harmful to national security. These activities, as reported by state-sponsored media, highlight the perceived dangers and threats that the VCSL aims to address and mitigate.

Cybersecurity is described as a matter of "network security, including ideological security, data security, technical security, application security, and capital security" that closely link to political security (Takong, 2014). This cybersecurity discourse is a typical national security approach that breeds the distinction between *legitimate* and *malicious*. Cybersecurity, therefore, is to draw the line between what is within and outside the sphere of legitimate activity (Shires, 2020).

Furthermore, state-sponsored media also accentuates this division by differentiating between various interlocutors with different political convictions (Van Dijk, 2008). Individuals engaged in behaviors deemed harmful to national security are labeled "hostile and reactionary forces," or "democratic, oppositional, political opportunists," with the intention of targeting the state, agencies and organizations, and other individuals.

Some foreign media agencies are also characterized as "black media," or "hostile media," as they "take advantage of the Internet to continuously spread a number of negative articles about Vietnam," or hold "unfriendly, one-sided and misleading views towards Vietnam," and "publish articles that are full of rhetoric with old tricks to provoke and disturb the media environment."

In addition to these reactionary forces, "irresponsible" and "uncivilized' social media users are also identified as contributors to cyber threats, posing a threat to the legal rights and

interests of agencies, organizations, and individuals. Many users opt to "use social networks in an anonymous form to slander organizations and other individuals, spreading a lot of negative and false information," or "post information on social networks without a sense of responsibility, causing negative impacts on social life, confusing people and damaging their dignity."

In accordance with the legal philosophy of national security (Q.-T.-T. Nguyen, Bui, & Phung, 2022) the state-sponsored media justifies that the VCSL "fully and timely institutionalize government policy and party line about cybersecurity and to ensure the appropriation with the 2013 Constitution about human rights." It is, thus, anticipated "to improve and eliminate gaps," as well as to "overcome limitations and existing problems related to network security protection" in the current legal corridor that have persisted over an extended period. Additionally, the promulgation of VCSL aligns with international agreements, and its "activities on information exchange."

The state-sponsored media signifies the VCSL as a legal framework aimed at facilitating and enhancing business operations in cyberspace by fostering "a fair competitive environment for both domestic and international enterprises," and "breakthroughs, development momentum for the economy and to utilize local's strengths." Furthermore, as highlighted, the law "brings in many more job opportunities for Vietnamese and strong partnership from investors." Simultaneously, it "strictly manages the activities of cross-border service providers when doing business in Vietnam; ensures payment sovereignty, prevents tax loss for these enterprises; at the same time, eliminates inequality in business activities between foreign enterprises and domestic enterprises."

International Media: The VCSL as a Threat. In stark contrast, international news media portrayed and scrutinized the promulgation of the VCSL, raising concerns about potential human rights violations, increased online censorship, and the imposition of barriers to business operations in the country.

Nearly 40% of the news corpus focused on significant international concerns related to human rights issues, while another 40% highlighted topics regarding data localization and content censorship. In contrast to national discourse that justified the law and legitimized the regime, international media revealed the underlying intentions of these new regulations, suggesting that they "targeting people who have the ability to mobilize their fellow citizens," "protecting the party's monopoly on power as to protect the network," and "providing yet one more weapon for the government against dissenting voices."

In their news coverage, international media outlets tend to reference relevant statements, reports, and events from organizations such as Human Rights Watch and Amnesty International, as well as human rights activists. The VCSL has been one of the most criticized and debatable subjects of intense criticism and debate, with representatives of various member countries and affiliated civil organizations challenging its provisions (Nguyet et al., 2022) at the Universal Periodic Review of the UN Human Rights Council for Vietnam in 2019. The VCSL's broad definitions of "evil" or "malicious" content, as well as its prohibition on offending and slandering the Party's leadership and its officials (Tran, 2017) have made criticism and freedom of expression intolerable and unacceptable to the VCP (Nguyet el al., 2022).

During the ICCPR hearing 2019, international delegates raised concerns about the VCSL, particularly regarding its abstract regulations and compatibility with international human rights standards. They also questioned the definition of legal and illegal content in cyberspace, the obligations of service providers in managing content based on authorities's requests regarding illegal content, the government's enforcement of limitations on freedom of expression through the law, and the negative impacts of the law on human rights (Nguyet el al., 2022). The law is justified in the name of protecting Vietnamese data privacy; however, it has been criticized for legalizing the government's surveillance to monitor individuals critical of the government (Phan, 2021).

International media cited the VCSL "has little to do with cybersecurity," as instead of prioritizing the identification and fixing vulnerabilities in computer systems, the party-state prioritizes policing online behaviors and surveillance of content (Woollacott, 2022).

Excerpt on international criticism (Syngergia Foundation, 2018) of the VCSL:

> International and local human rights activists have noted that the law could be used to silence dissenters. Human rights group Amnesty International noted that the law would give sweeping new powers to the Vietnamese authorities, allowing them to force technology companies to hand over potentially vast amounts of data, including personal information, and to censor users' posts.

Rationalization of Cyber Threats on State Media

To further analyze how state-sponsored media exemplify cyber threats in their discourse to justify the enforcement of the VCSL, this part discusses the presentation of various types of threats.

In the national news corpus, a substantial portion, comprising over one-fifth of the entire text data, is dedicated to topics concerning cybersecurity threats. These threats can be classified into two main types, human-related and technique-related risks, each encompassing distinct sources, goals, and means (Sharikov, 2019).

Human-related threats are attributed to human actors engaging in *illegal* and *prohibited acts* (means) such as *cyber espionage, terrorism, anti-state, theft, misrepresentation, fraud, incitement, distorting history, denying revolutionary achievements* targeting party-state on endangered values (goals) such as *national sovereignty, national security, national defense, unity bloc,* and *state secrets*. These human actors (sources) are labeled as *hostile forces, reactionary forces,* and *cyberespionage*.

Besides, there are other threats that affect individuals and public well-being (goals) including *social order, legitimate rights of individuals and organizations, fine custom, custom*

tradition, and *revolutionary achievement*. These threats are brought about by *malicious* internet users and *hi-tech criminals* (sources) through harmful behaviors (means) such as *personal information theft, fraud, property appropriation, slander, humiliation, libel attacks, restriction of malicious code, gradual elimination of acts gambling, betting, propagating depraved cultural products, inciting violence, prostitution and other illegal acts in cyberspace*. It is worth noting that threats caused by human actors are usually interconnected and intertwined with other topics, typically signaled by keywords such as *prohibit, violate,* or *attack*.

Meanwhile, the country is currently facing four common types of technique-related cybersecurity threats, namely denial of service, interface-changing attacks (deface), phishing, and malware (Le, Nguyen, & Ngo, 2020). These threats specifically target *personal data* and *information systems* of *businesses, banking and financial institutions,* and *state agencies*. To be more specific, these attacks involve *phishing campaigns by using e-mails containing ransomware, scamming users through malicious links, skin-changing attacks, spreading computer viruses…*

In the security protection mechanism, the priority of endangered values is ranked according to the level of importance. Lawful rights and interests of individuals and organizations are considered the lowest priority (grade 1 and grade 2), followed by public interests and social order (grade 2, 3, and 4) at a moderate level, and national defense and security as the highest (grade 3, 4, and 5). The highest priority is given to national defense and security (grade 3 to grade 5), where any sabotage of an information system can cause harm or extremely serious threat to national defense and security (Romaniuk & Manjikian, 2021)

Cybersecurity is viewed from both political and legal aspects (Vu, 2019), with national security being regarded as the first and foremost priority, even surpassing the security of information infrastructure itself or human rights (Wagner, Kettemann, & Vieth, 2019). In Vietnam's case, national security holds even greater significance as it ensures the security of the Communist Party, which is considered as the sole "force leading the State and society"

(Lesmana, 2016). The frequency of top five collocates of *security* indicate the primacy of *national security* (722 instances) over *network security* (614 instances) and *information security* (396 instances).

To justify the implementation of new regulations and increased surveillance measures on Internet users and foreign telecommunication operations within the country, the state and state-sponsored media have employed hypersecuritization practices with an emphasis on "multi-dimensional cyber disaster scenarios" in almost every news article to create a sense of urgency (Hansen & Nissenbaum, 2009). By portraying potential cyber threats and their potential consequences in an exaggerated manner, they seek to highlight the need for stricter regulations and surveillance to protect national security and stability. This approach aims to evoke fear and generate public support for the implementation of these measures.

To emphasize the severity of cyber attacks on the national information and network system, state-sponsored media portrayed the country as "top 10 countries hit by distributed denial-of-service (DDoS) attacks in the last quarter of 2017," "top 10 countries controlled by ghost computer network in 2018," "ranked 20th among the countries in the world where the network system is attacked by malware," "ranked 8th among the top 10 countries in the world in terms of local malware infection." In addition, to highlight the economical consequences of cyber attacks, national media repeated "in 2017, the damage caused by computer viruses to Vietnamese users reached 12,300 billion VND (540 million USD)."

The state-sponsored media, subsequently, navigate threats from national level to individual scenarios.

> There are stories of many individuals having to inform each other about being "hacked" and having their online interfaces manipulated. There are also numerous scams by "invisible" perpetrators lurking day and night, aiming to steal collective and personal assets. Even private secrets and personal relationships have been exposed online, disrupting and impacting many people's lives. Some individuals, driven to despair, have tragically taken their own lives.

This kind of securitization discourse connects global threats right down to personal safety, even death and stability of technical and social aspects that are designated vital to collective life (Tikk & Kerttunen, 2020). This discourse is particularly fitting for a country with strong collectivist values like Vietnam. These threats are described as ongoing, existing incidents, despite the absence of real and significant events. This aligns with the nature of securitization scholarship, which often deals with the amorphous and ambiguous characteristics of national security (Tikk & Kerttunen, 2020).

In the face of these prevalent cyber threats, national media organizations reinforce the mission of the state and government in protecting endangered values through *crime prevention* and enhancing *security protection,* and *defense security*. Consequently, the VCSL serves as a *legal basis, a legal corridor* to *prohibit acts, handle violation, serve investigation*, and *raise awareness*.

The law is also signified as a driving force for *digital transformation* and the *industrial revolution*. The strong emphasis on cybersecurity threats, subsequently, is to justify the increased surveillance on online content, which aligns with the surveillance-as-regulation approach (coupled with the censorship-as-regulation approach) adopted by state actors. This approach was formulated as a response to collective opposition from non-state and hybrid actors during the period of extensive public resistance against the draft law of VCSL in June 2018 (H. N. Nguyen, 2022).

Divergent Media Presentations on Cybersecurity and Human Rights Issues

While national media portrayed human rights concerns as an ideological reinforcement to justify the VCSL, international news media provided ongoing reports on real-life instances of human rights violations in the country, along with public criticism of controversial regulations. This disparity reflects the contrasting perspectives and priorities of national and international media outlets when it comes to human rights discourse.

State-sponsored Media: Human Rights as an Ideological Reinforcement.

Approximately one-third of the national news corpus mentioned legitimate and lawful rights and interests of individuals and organizations. The emphasis on the topic reflected the state's prompt responses to public reaction and debate surrounding the introduction of the VCSL. The drafting of the law raised concerns and provoked anger among many people, as they perceived the proposed regulations as infringing upon fundamental human rights, especially personal privacy, freedom of expression, freedom of speech, and press freedom.

The public discontent manifested in demonstrations across more than 10 cities in Vietnam in mid-2018. Given this context, the extensive media coverage on human rights issues not only aim to address both public and international concerns but also to increase the legitimacy of the law and regime. Amidst oppressed dissident voices and international criticism, the state and state-owned media have undertaken extensive efforts to substantiate the existence of human rights in the country.

National media discourse on human rights topics has two main focuses.

First, national media strategically reinforces the mission of the VCSL in ensuring legitimate and lawful rights of individuals and organizations, while carefully balancing these rights with national security concerns. In the discourse of national media, the term '*rights*' is often collocated with positive descriptors such as *legitimate, lawful, social, international, universal, political, basic,* and *fundamental* which indicates the party-state's acknowledgment of the fundamental importance of human rights within the context of cybersecurity governance.

Excerpt on VCSL's protection of human rights:

> The Law on Cybersecurity protects the right not to be infringed upon personal honor or reputation, which prohibits acts that may infringe upon the honor or reputation of others, and at the same time protects the right to freedom of thought, belief, and citizens' religion. The law also

protects citizens's right to freedom of speech and expression. (The World & Vietnam Report, 24 September 2021)

By employing a hypersecuritization strategy, the state-sponsored media highlight the critical importance of the VCSL's enforcement to *protect* and *ensure* those lawful rights from "humiliation, slander that seriously offends the dignity and honor; fabricated or untrue content in the fields of finance, banking, e-commerce, electronic payment, currency trading, capital raising, multi-level business, securities; untrue information causes confusion among the people; and loss or change of information belonging to personal secrets, family secrets, and private life are transmitted and stored in cyberspace."

The tactic to emphasize benefits and resources associated with the VCSL aims to secure the regime legitimacy by instilling a sense of security and protection among the populace, thereby garnering continued and long-term acquiescence from active supporters. This strategy is commonly employed by authoritarian governments, especially when facing foreign criticism (Babb, 2022) or during periods where factors that could challenge the legitimacy of the regime or ruler emerge (Geddes, 1999).

	National news	International news
Nouns	human, interests, citizens, organizations, safety, individuals, children, covenant, security, freedom, constitution	human, Vietnam, Watch, groups, activists, freedom, defenders, Asia, Amnesty, organizations, government, users, companies, interests, standards, violations, authorities, concerns, dissidents, activism, criticism, advocacy, crackdown, brutality,
Verbs	protect, ensure, exercise, infringe, violate, exploit, hinder, attack	abuse, protect, violate, respect, arrested, promote, sentenced, defend, undermine, imprisoned, jailed, condemned, intimidate, demonstrates,

Adjectives	legitimate, lawful, social, international, universal, political, basic, fundamental	notorious, unlawful, worsening, abysmal, enshrined, regressive

Table 7. Annotation of the Most Frequent Collocations of *Rights* in the National and International News Corpora

Despite the party-state's continuous assertions that human rights in the country are natural, inherent, and protected by the Constitution at the highest possible level, they are predominantly perceived as state-granted rights (Bui, 2022). These rights cannot be separate from duties, citizen's fulfillment of their obligations towards the state and society (Constitution of Vietnam, 1992) and are restricted in the state of emergency to protect national security, public order, and social health and morality (Bui, 2022).

This statist approach to human rights aligns with the post-reform and communitarian concept prevailing in the country, which places a greater emphasis on economic and social rights at the expense of political and civil rights (Bui, 2022). Therefore, secondly, national media also focused on delineating boundaries of these legitimate rights to prevent the abuse of democracy and freedom of speech, particularly in ways that would encroach upon at least 7 bottom lines (Luong, 2022) under Article 8. These principles include: the rules and laws of the country, the socialist system, the country's national interests, the legitimate interests of the citizens, public order, morality, and authentic information.

To increase legitimacy of the law, national media claimed that the law is "not a tool for the State to prevent free speech like what the 'bad guys' intentionally put forth", (Vietnam Plus, 2018) and "the state always respects and facilitates the rights of its citizens to exercise freedom and democracy but also against the abuse of those rights to commit illegal activities." (Vietnam News, 2018).

Therefore, "the law is not to violate but facilitate human rights such as freedom of speech and freedom of expression… Everybody has the right to express personal opinion but we must

abide by the law, we cannot do whatever we want to in the name of freedom" (Kiem Sat Online, 2020). The law, thus, only aims to "adjust relationships among citizens, between citizens and society, and between citizens with the state." Some media outlets also claimed, "in the face of the turbulence on social networks recently, the law should have been introduced even earlier" (Vietnam Plus, 2022).

International Media: Human Rights Violations as Real-life Events. There is 37% of text data in the international news corpus focused on human rights issues. Foreign media outlets not only featured comments and letters from international organizations such as Human Rights Watch, Reporters Without Borders, and Amnesty International calling for the law repeal but also provided updates on demonstrations, tensions between local government and protesters, and the situations of arrested protesters, journalists, and activists who faced persecution during the promulgation and enforcement of the VCSL. Foreign media described new regulations as *notorious, unlawful, worsening, abysmal,* and *regressive*.

Excerpt on international media (South China Morning Post, 2019) criticism of the VCSL:

> "This law is designed to further enable the Ministry of Public Security's pervasive surveillance to spot critics, and to deepen the Communist Party's monopoly on power," Phil Robertson, deputy Asia director of HRW.

Contrary to the portrayal in national media, the introduction of the VCSL at the 14th National Assembly received negative feedback and dissent from citizens. Beyond petitions calling for the withdrawal of the bill, at the peak of the movement, there were demonstrations and gatherings, some of which involved occasional violence, in at least 10 different cities to oppose the special economic zone and cybersecurity law bill in mid-2018. International media used mostly negative tones and strong verbs when referring to these events such as *abuse, violate, arrest, sentence, defend, undermine, imprisoned, jailed, condemned, intimidate,* and *demonstrate…* which leave *devastating consequences* to the people, human activists, and the

whole country. However, state-sponsored news coverage often omitted or downplayed these events, providing limited information about the dissent and the reactions it elicited.

According to international coverage, the VCSL is "to allow authorities to restrict free speech," "bad news for human rights activists," "critical expressions are under threat," "help the Vietnamese regime to silence its critics," and, thus, "has potentially devastating consequences for freedom of expression." In stark contrast, national media portrayed the VCSL as an outcome with "a high approval rate after going through multiple rounds of discussion and open, transparent consultations involving lawmakers, experts, businesses, and the general public" (VN Express International, 20 July 2018). They emphasized the transparency, legitimation of the law ratification process, and the high level of consensus from the public. This was reflected in the repeated use of certain words such as the *National Assembly listened, voted, approved*, and *passed*.

At the later stage of the VCSL enforcement, international organizations continued to cover arbitrary censorship, surveillance measures, and authority's intimidation over land disputes in Dong Tam and Covid-19 information in 2020 in the country.

> Between January and mid-March, a total of 654 people were summoned to police stations across Viet Nam to attend 'working sessions' with police related to their Facebook posts connected to the virus, among whom 146 were subjected to financial fines and the rest were forced to delete their posts." (Amnesty International, 2020)

The arrests mainly fall under regulations of "conducting propaganda against the state" or "abusing democratic freedom." For example:

> On 18 April, authorities in Hau Giang province arrested Dinh Thi Thu Thuy, 38, for 'conducting propaganda against the state' under Article 117 of the 2015 Penal Code. Separately, on 12 April, police in Can Tho city arrested and detained Ma Phung Ngoc Tu, 28, for 'abusing democratic freedom' under Article 331 of the 2015 Penal Code. Police accuse Ma Phung Ngoc Tu of

'posting and sharing 14 posts about coronavirus and bad-mouthing the regime. (Amnesty International, 2020)

Cybersecurity as Momentum for Digital Transformation Versus Data Localization as Business Barriers

Besides human rights issues, data localization is another contentious topic that covered one-fourth of data text in the national news corpus and nearly one-fifth of that in the international news corpus.

State-sponsored Media: Cybersecurity as Momentum for Digital Transformation. According to state-sponsored media, the VCSL regulations, particularly regulations on data localization, are presented as having no side effects but rather only strengthen security for the business environment and boost digital transformation in the country. The media claims that these regulations create "a fair competitive environment for both domestic and international enterprises," "breakthroughs, development momentum for the economy and to utilize local's strengths" and "many more job opportunities for Vietnamese and strong partnership from investors" (Vietnam Plus, 2018).

Excerpt on benefits of VCSL on business development:

… This regulation also creates a legal corridor for functional ministries and branches to strictly manage the activities of enterprises providing cross-border services when doing business in Vietnam; ensure payment within sovereignty and prevent tax loss for these enterprises; at the same time, eliminate inequality in business activities between foreign enterprises and domestic enterprises. (Vietnam Plus, 2018)

Regarding public concern on data localization regulation and its consequences, national media corrected: "It is unlikely that the VCSL will seriously damage the Vietnamese economy, or that Vietnamese businesses will fail due to the provisions of the law" and "the network

operators do not object, do not intend to withdraw from business investment in Vietnam as misrepresented by hostile forces" (Tay Ninh Online, 2021). They also confirmed the law "will not generate sub-licenses, hindering the development of businesses, but on the contrary, it can also reduce costs if businesses set up content servers in Vietnam," and "does not require companies to store all Vietnam-related cyber data or platform data but only specific data relating to personal secrets in emergency cases and national security." As a result, the law only aims to "provide favorable conditions for foreign businesses and investors to operate in Vietnam."

Furthermore, national media denied accusations of state control over user data being labeled as *power abuse*. They resisted "if law implementers abuse their power to violate citizen's and enterprise's rights, they will be punished. There is absolutely no power abuse here" (Viet Nam Plus, 2018).

International Media: Data Localization as Business Barriers. Opposite to national media's generic language to highlight the benefits of data localization, international media delved into the in-depth analysis of its consequences with two main issues.

First, international media responded that the VCSL's concept of data localization, which is used to legitimize local data storage requirements within territorial jurisdiction, is actually "cyber paternalism" or "data nationalism"(Quinn, 2017). Countries that deploy such strategy either intentionally misuse or unintentionally misunderstand the nature of data security as:

> …The security of data is not determined by the location in which it is stored, but by the technical, operational, and managerial practices implemented to secure it. Data localization laws can restrict cost-effective access to state-of-the-art and secure global information technology services, including software service providers and cloud service providers. (Nikkei Asia, 2022)

According to international media, data localization is seen as contradictory to the free and open nature of the internet, as it hinders the cross-border supply of services and disrupts global data and cybersecurity operations for foreign companies (Beattie, 2018), and creates business

obstacles as it could "deter innovation, limit consumer choice and raise market entry barriers, particularly for Vietnamese entrepreneurs," especially, for small and medium enterprises. These obstacles include high operation costs associated with maintaining local servers and representative offices, concerns about data privacy concerns, and security risks relating to the reliance on government-designated third-party companies or low-security domestic facilities.

> …Free cross-border flows can harness data analytics and create the best possible ecosystem for local businesses to use digital technologies and thrive internationally. Currently, small and mid-sized enterprises that lack an international footprint rely on the free flow of data across borders to make use of common infrastructure to serve customers in different markets. Data localization requirements will raise the cost of doing business for these SMEs. (Nikkei Asia, 2022)

More importantly, regulations on data localization are considered to be in violation of international trade agreements that Vietnam has ratified, including the 11-Country Comprehensive and Progressive Agreement for Trans-Pacific Partnership (TPP-11), Vietnam-EU Free Trade Agreement (EVFTA), and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Under these agreements, signatories are not allowed to dictate whether or not a company can conduct business based on where its IT infrastructure is located (Nikkei Asia, 2018). Therefore, the new regulations on data localization are seen as digital disasters that "undoubtedly hinder the nation's fourth industrial revolution ambitions to achieve [gross domestic product] and job growth;" (Nikkei Asia, 2018) and "a Vietnam that shuts itself off from global data flows is a Vietnam that shuts itself off from global growth" (The National Interest, 2018).

Second, international media also see data localization as a form of disguised protectionism (Mishra, 2020) that not only results in increasing cybersecurity vulnerabilities and the cost of doing business (Nikkei Asia, 2022) but also human rights violations as it legalizes and legitimizes state surveillance on personal and business data by turning technology companies operating in the country into de-facto state surveillance agents (Nikkei, Asia, 2018).

> …By requiring data localization and local offices, the Hanoi government is demonstrating that its disregard for human rights can also be bad for business. As the Asia Internet Coalition stated, the law would undoubtedly hinder 'the nation's 4th Industrial Revolution ambitions to achieve GDP and job growth. (Asia Sentinel, 2019)

Regarding Facebook's compliance with the government's demands on content removal, foreign media referenced Amnesty International:

> Facebook's compliance with these demands sets a dangerous precedent. Governments around the world will see this as an open invitation to enlist Facebook in the service of state censorship.

and activists:

> …Duy Hoang, the spokesman for Viet Tan, an unsanctioned Vietnamese pro-democracy party said, 'the so-called cybersecurity law does nothing to protect internet users.' It's a blatant effort by the Vietnamese government to crack down on online expression by enlisting the help of Western technology companies such as Facebook and Google.

Media Presentations Within Linguistic Construction: Us Here Good, They There Bad

Heavily based on performance and procedure-based legitimacy, the Vietnamese government is sensitive to foreign criticism. In their coverage of the VCSL, both state-sponsored and international media not only exhibit distinct priorities and frames but also engage in a reciprocal dialogue, either through direct or indirect responses to each other's discourse. This final section of the discussion aims to examine the utilization of various linguistic features by these media actors to engage in confrontational and antagonistic narratives.

In response to criticism from international media, the state and state-sponsored media employed both defensive and offensive strategies. Defensively, they sought to shield their accounts from rival attacks by reinforcing their legitimacy and credibility (Potter, 1996; Tileagă,

2012). Offensively, they aimed to reshape audience attitudes and alter beliefs about the accused's responsibility for certain actions, effectively undermining rival narratives (Benoit, 2015). This dual approach serves to both protect and promote their version of events, ensuring control over public perception and discourse.

There exists a clear opposition and competition in media discourse between national and international media outlets regarding cybersecurity issues in general and the VCSL in particular. In the national news corpus, on the one hand, national media bolster the VCSL, legal corridor, and the protection of citizen's rights with positive adjectives such as *legitimate, lawful, fundamental,* and *comprehensive*. Furthermore, state actors are also assigned with active verbs such as *protect, ensure, strengthen, stipulate, deploy,* or *combat* to emphasize the mission and importance of the VCSL enforcement. On the other hand, when addressing *hostile media* or *reactionary forces*, national media tend to portray them as *illegal, dangerous*, and *false*; and such subjects would *infringe, take advantage of*, and *disrupt* endangered values such as *national security, legitimate rights, social order*, or *state secrets*.

Besides rationalizing and bolstering the VCSL, national media also responded and defended the law directly in the face of international criticism. For example, regarding law regulations that are deemed to violate human rights, Aljazeera (2018) stated:

> The new law will prohibit users from using online for anti-state purposes, spreading false information, or taking part in online activities that potentially undermine the country's achievements or solidarity. In response, the human rights organization Amnesty International called the new law 'deeply regressive...' With the sweeping powers it grants the government to monitor online activity, this vote means there is now no safe place left in Vietnam for people to speak freely.

The state-sponsored media responded:

> Some foreign media agencies take advantage of the Internet to continuously spread several negative articles about Vietnam, some news agencies also publish articles full of rhetoric with old tricks to provoke and disturb the media environment.

And,

> Like the previous common motif of many political opportunistic, domestic and international forces, they took the name of 'democracy, human rights,' 'freedom of speech,' and 'freedom of the press' to transform information aimed at slandering, fabricating, and belittling the role, position, and prestige of the Party and State. The depth of these acts is to form and gather forces to oppose and overthrow the government.

In another news article, RFA (2018) cited statistics:

> According to Paris-based media watchdog Reporters Without Borders' 2018 World Press Freedom Index, Vietnam ranks 175th out of 180 countries and currently jails 25 professional and citizen journalists. Rights group Amnesty International estimates that at least 97 prisoners of conscience are currently held in Vietnam's prisons, where many are subjected to torture or other ill-treatment.

National media directly questioned foreign media's legitimacy:

> Do the comments, assessments, statistics, analyses of the BBC, RFA or VOA truly and objectively reflect the issue of press freedom in Vietnam? Or these are just old tricks of hostile forces to deliberately distort, smear, and discredit the country?

The state media challenge the authority of these organizations by explicitly indicating that they are self-claimed. For example, the state media asserted that RSP "gave itself the right to promote freedom of the press and freedom of expression in the Western style. RSF is a name with no face that often distorts and distorts the situation of press freedom in Vietnam." Additionally, they stated, it is clear that the Freedom House has no rights to intervene into the internal affairs of countries. It must immediately put an end to such valueless reports."

Furthermore, the state media not only discredit the "so-called" annual reports of these organizations but also disqualify their comments and assessments as "misleading, lacking in objectivity, even distorting the issue of press freedom in Vietnam," and "again contains prejudiced and partial assessments on internet freedom in Vietnam. Such assessments have no valid grounds and intentionally ignore the vivid reality of internet freedom in Vietnam, as well as achievements the country has recorded in human rights over the past years."

They also argue:

> The Freedom House has repeatedly made biased and prejudiced assessments on Vietnam's internet freedom since the country issued the VCSL. It mainly collects such information from reactionary organizations and groups that are involved in activities to sabotage Vietnam. The fabricated information aims to create false understanding on internet freedom and human rights in Vietnam, to defame the country and lower its prestige, position and role in the international arena.

The state-sponsored media question,

> Do the comments, assessments, statistics of the RSF or the articles, analyzes and comments of the BBC, RFA or VOA really and objectively reflect the issue of press freedom in Vietnam? Or these are just tricks of forces hostile to Vietnam, deliberately distorting to smear and discredit Vietnam? For the purpose of inciting and opposing Vietnam, the above organizations only mentioned and emphasized the rights to freedom of journalism, freedom of press, freedom of speech in the press without mentioning the right to be protected in a fair and ethical manner in the press and media. They also deliberately did not mention the role of law in regulating press activities for the common purpose, harmony of society and people's welfare.

To lend more credibility to these statements, the state media referenced an international source, Professor Vladimir Kolotov, head of the Ho Chi Minh Institute at St. Petersburg University in Russia, who said "the reports issued each year by Freedom House neither base on realities nor reflect the real situation of human rights in countries. It gives itself the right to

accuse other countries of violating human rights and interfere into other countries' internal affairs."

The distinction between us and them in cybersecurity discourse has become considerably more prevalent after the 9/11 incident to refer to terrorism attacks on, particularly, Western society, values, and morals (Bowman-Grieve, 2015). The contrast between us here good and they there bad or the legitimization of us and delegitimation of them is common in political discourse. This construction or reliance on a specific ideological narrative to increase regime's legitimacy often goes hand in hand with the demonization of foreign entities by labeling these threats (Babb, 2022). One needs to establish its legitimacy or "right to be obeyed" through positive-self (e.g., self-praise, self-justification, self-explanation) and negative-other (e.g., blaming, scape-goating, marginalizing, denying) presentation as a source of authority, reason, vision, and sanity (Chilton, 2004). Compared to other types of authoritarian regimes, single-party regimes are the most active ones in using tactics to legitimize their rule, prop themselves up, and delegitimize their rivals (Dukalskis & Patane, 2019).

5.5. Reflection on SJT

Findings of the Study 1 elucidate the significant role of existential threats, outcome dependence, and the power of status quo maintenance in shaping public perception and justifying political arrangements. The Vietnamese case illustrates how these psychological mechanisms are strategically employed to garner support for contentious laws and policies. By presenting cybersecurity threats as existential risks, emphasizing the positive outcomes of the VCSL, and framing the law within the context of maintaining stability, the party-state strives to sustain its legitimacy and control.

Existential threat is a central tenet of SJT, positing that individuals' motivation to justify and defend the status quo intensifies when they perceive their social system as threatened. This study demonstrates how state-sponsored media in Vietnam leverage this principle by framing cybersecurity threats as imminent dangers to national security, societal order, and individual

safety. This aligns with the theoretical assertion that under conditions of threat—such as terrorism, climate change, economic downturns, and natural disasters—peoples's drive to reinforce the legitimacy of the existing system becomes more pronounced (Friesen et al., 2019). Empirical studies have shown that priming individuals with threats to the economic or political system significantly increases their support for the status quo (Kay, Jost, & Young, 2005; Lavitan & Jost, 2014). By emphasizing existential threats, the media not only aim to unify public perception around the necessity of stringent cybersecurity measures but also minimize resistance by framing these measures as essential for survival and stability.

Outcome dependence refers to the extent to which individuals rely on the system for their well-being and security. This study reveals that state-sponsored media in Vietnam project the VCSL as a crucial framework ensuring positive outcomes, from enhanced security and social order to economic growth to guaranteed security and rights and interests of individuals. By highlighting the beneficial impacts of the VCSL, the media create a perception of dependence on the system, thereby fostering greater acceptance and justification of the law. This strategy resonates with findings from previous research indicating that increased dependence on a system enhances perceived legitimacy and support for the status quo (van der Toorn et al., 2011). For instance, studies have shown that individuals who perceive themselves as highly dependent on governmental systems are more likely to view government policies as legitimate and necessary (Kay et al., 2009). The state media's narrative effectively taps into this psychological mechanism, making citizens more inclined to view the VCSL as a necessary and beneficial regulation.

The maintenance of the status quo is a powerful force in system justification. The findings demonstrate that state-sponsored media in Vietnam leverage the idea of the status quo by emphasizing the longstanding and traditional aspects of the current political system. By presenting the VCSL as a continuation of Vietnam's commitment to security and stability, the media reinforce the perception that the existing system is both natural and beneficial. This strategy aligns with the notion that people are more likely to justify and rationalize systems perceived as stable and unchangeable, as it reduces cognitive dissonance and promotes a sense of

order (Jost, 2020a). Research has indicated that individuals are more likely to support new policies once they are implemented and perceived as part of the status quo (Laurin et al., 2012). Furthermore, by comparing national and international media discourses, the study highlights how the state uses media to frame cybersecurity laws in a way that minimizes dissent and fosters compliance, thus maintaining the status quo.

This analysis underscores the broader implications of SJT in authoritarian contexts, where state actors can manipulate existential threats and outcome dependence through media control and censorship to reinforce the maintenance of status quo. It also highlights the importance of examining media discourse as a tool for understanding how governments justify their actions and policies to the public. The study's findings contribute to a deeper comprehension of the dynamic interplay between psychological motivations and political communication in shaping public attitudes towards state authority and regulations.

In authoritarian regimes, the continuous emphasis on national threats and the necessity of state-led interventions create a narrative that aligns public perception with government policies. Studies have shown that in China, similar strategies are used to justify stringent internet regulations under the guise of national security, and to convince local states, market actors, intellectuals, as well as the general public (Zeng, 2021).

The sophisticated application of SJT in this study not only reinforces the theory's validity but also provides a nuanced understanding of the intricate mechanisms through which state-sponsored media shape and sustain the legitimacy of the ruling regime in Vietnam. The empirical findings from this research, supported by evidence from other authoritarian contexts, underscore the powerful role of media in constructing and perpetuating system-justifying narratives, particularly under conditions of perceived existential threat, outcome dependence, and the inherent power of status quo maintenance.

Chapter 6. The Positioning of Us, Them, and the Powerful Leadership of the Party-State

6.1. Research Objectives and Research Design

The Study 2 adopts an institutional approach to investigate dispositional attributes by analyzing factors that might trigger cognitive motives for system justification through the positioning of self and others, and stance-taking. Specifically, the study aims to analyzing the portrayal of citizens as powerless in the face of cyber threats and political dynamics; investigating the promotion of political allegiance to the VCP as a fundamental aspect of responsible citizenship; examining the alienation and demonization of hostile forces to legitimize the marginalization and suppression of dissent; examining constructed rights and obligations of involved. According to SJT, individuals experience a sense of powerlessness towards existential threats, leading to allegiance and alienation and, consequently, acceptance and justification of socio-political arrangements that satisfy their need for closure and strengthen their national or group identity and political allegiance.

The intersection of language, power, and ideology (Fairclough, 2010) in media discourse provides a foundation for examining how state narratives shape public perception and maintain political control. This study combines CDA with Positioning Theory as a supplemental theoretical framework to offer a robust methodological framework for uncovering the mechanisms through which these narratives are constructed and perpetuated. The study not only analyzes dispositional attributes that motivate system justification but also through the analytical process to investigate how different actors are positioned and have their identities constructed. This involves an analysis of *us*, potential victims of cyber threats and lawmakers (the party-state) who will protect *us*, as well as security subjects like *them*, who threaten existential needs or oppose the law. Furthermore, the study examines the government and VCP's stance in regulating cybersecurity through their evaluation of referent objects and their alignment or disalignment with other stakeholders's stances.

In this study, state-sponsored media discourse, representing the state-party's mouthpiece, is analyzed as an ideological competence, in relation of moral standing (Langenhowe & Harré, 1995), and struggle for power and hegemony among different media actors through language, institutional practices, subjectivity, and power that constitute their discursive structure. Self-positioning and subject positioning are constructions of this process, where narrators distinguish and position themselves (us) from the others (them) to obtain meaning by being attached situationally to certain categories and storylines (Törrönen, 2001). Discourses and storylines are inherently social and cultural constructs; therefore, the positions they entail cannot be fully comprehended without referring to D-discourses (Foucault, 1969) and the associated rights and duties of characters within these narratives (e.g., Davies and Harré, 1990; Harré and van Langenhove, 1991). In other words, as positions are tied to social actions, investigating positioning in narratives allows understanding of how people accomplish situated identities (Fina & Georgakopoulou, 2015).

Subject position also evolves in an interactional relation with the audience and existing subject positions in a particular context (Törrönen, 2001). Examining self and subject positions helps shedding light on the social motives of speakers and their distinctions of what is rational versus irrational, legitimate versus illegitimate; what kinds of social relationships are trusting and honorable versus secret, suspicious, and self-interested; and what kinds of social institutions are considered rule-regulated, contractual, and equal versus arbitrary, class prejudiced, and hierarchic (Alexander, 1998, as cited in Törrönen, 2001).

The study also examines positioning as part of the stance-taking process as it has a broader meaning including both positioning of self and others, evaluation of objects, and alignment or disalignment to objects and other subjects (Berlin, 2020). Stance in discourse is a relational concept. Stancetaking involves reacting to or positioning oneself relative to something else, typically a message or topic (Du Bois, 2007). "Stance" generally refers to a speaker's attitude, emotional expressions, desires, and expressions of beliefs and certainty toward specific issues, people, or paradigms (Haddington, 2004). While positioning emphasizes the speaker's

role in manipulating the input through language use, stance focuses more on the resulting overall image, shaping the interpretation of the hearer or receiver (Berlin, 2020). The examination of stance taking does not only provide understandings on resonances of juxtaposed utterances in discourse (Du Bois, 2001) but also construct stances by engaging with, modifying, building upon stances taken (Du Bois, 2007; Haddington, 2005), as well as alignment as the act of calibrating the relationship (Jaffe, 2010) between speakers and stance-takers.

The study also applies Du bois' model to examine the stance-taking process in cybersecurity discourse study. Evaluation is the most salient and widely recognized form of stance taking, wherein a stance-taker orients to an object of stance and characterizes it as possessing a specific quality or value (Du Bois, 2007). Evaluation implies self-expression that is directed toward a narrow scope, specifically, self-expression about "entities or propositions" (Thompson & Hunston, 2000). In this process, securitizing actors (including state and non-state actors) define and evaluate referent objects (traditional or non-traditional security values) as well as other subjects through alignment or disalignment with them to socially construct positions of self and others to later justify their acts.

6.2. Research Method and Materials

In light of SJT and Positioning Theory as a primary theoretical framework, this research adopts a qualitative approach, employing CDA focusing on an analysis of positioning and stance-taking (Du Bois, 2007). This study reuses the news articles in the "National News" dataset in the previous study.

CDA is particularly suited for this study as it allows a nuanced examination of how media discourse serves to uphold and legitimize political authority. CDA shows that media texts function in dual capacities: as representational tools that construct and mediate social reality, and as interactive mechanisms that shape the social identities and relationships of participants in a communication act (Fairclough, 1995).

The CDA component of this research is structured around three core themes: the positioning of lay people as powerless in contrast to the powerful leadership of party-state, the promotion of political allegiance to the VCP, and the alienation of hostile forces, the construction of rights and obligations for involved parties. Each theme is examined through several analytical lenses to uncover the linguistic and rhetorical strategies used in media discourse.

An examination of lexical choices is critical in the analysis. This involves analyzing the specific words and phrases used to construct narratives around powerlessness, political allegiance, alienation, and rights and obligations. For instance, terms such as *protection, guidance, and supervision* are often employed to describe citizens, reinforcing their perceived need for state intervention. Similarly, words like *lawful, patriotism,* and *duty* are used to frame political allegiance, promoting the idea that support for the VCP is synonymous with true patriotism. The study also examines modality, focusing on the use of modal verbs like *must* and *should*, as well as other grammatical structures that emphasize necessity, obligation, and inevitability. This analysis reveals how language constructs a sense of urgency and inevitability around compliance with state policies, suggesting that such compliance is both necessary and unavoidable.

Through a scrutinization of lexical choices, it is revealed how state media texts explicitly position actors in specific roles and identities. This involves identifying how citizens are portrayed as dependent on state protection, the VCP is depicted as the legitimate authority, and hostile forces are characterized as threats. By positioning citizens as reliant on the state for security, the media reinforces the notion of the VCP's indispensability. Similarly, by casting hostile forces as threats, the media justifies the state's stringent measures and delegitimizes dissent.

Moving beyond lexical examination, the study investigates the broader framing and rhetorical strategies used to reinforce state narratives. This includes identifying how issues are framed in ways that support the state's ideological positions as well as how patriotic rhetoric,

moral framing, and cultural values are being used to invoke national pride, moral duty, and cultural identity among citizens. For example, as moral positioning is an important rhetoric tactic of the party-state, the study delves into the moral attributes and responsibilities assigned to different actors, reinforcing or challenging power dynamics. This involves examining how citizens are morally obligated to comply with state policies, how the state positions itself as the moral guardian of national security, and how hostile forces are morally condemned. By attributing moral responsibility to compliance, the media constructs a narrative where supporting the state is not only a civic duty but also a moral imperative. Conversely, by morally condemning hostile forces, the media delegitimizes opposition and frames dissent as inherently unethical.

Dialogicality, or interactional nature of stance-taking (Du Bois, 2007) is another critical tenet that needed to be investigated in this study. Alignment or disalignment strategy demonstrates the connection between speakers and interlocutors, showing whether they echo the stances of previous or distal interlocutors (Pinto-Coelho et al., 2019). As the Study 2 only examines the state-sponsored media discourse, it explores how the party-state reflects, responds, accepts, resists, or negotiates other arguments in its narratives. For example, the study analyzes the media's portrayal of public reactions to state policies and the VCSL, as well as any evidence of resistance or compliance. The study looks at how the media represents the public's response, whether supportive or oppositional, and how these portrayals influence the perception of state authority. This aspect of positioning theory reveals the dynamic interaction between the media and the audience, highlighting how discourse can reinforce or challenge power relations.

Through these three aspects of positioning, the research uncovers how Vietnamese state media constructs and negotiates the roles and identities of various actors within the discourse. This comprehensive analysis reveals the complex interplay of language, power, and ideology in maintaining the status quo and legitimizing state authority.

6.3. Findings and Discussion

Using state-sponsored media as the state-party's mouthpiece, the government strategically manages the impressions others have of them while establishing their own legitimacy (van der Toorn et al., 2015). The media delineate different agentive characters, classifying them into two main groups, *us* and *them*.

Us is further divided into two subgroups: the authority and the powerless. The powerful *us* include the party and the state, security actors at the highest level, and institutionalized government bodies such as the Ministry of Information and Communications, Ministry of Public Security, Ministry of Education and Training, Ministry of Culture, and Ministry of National Defense. The powerless *us* refers to laypeople or the general populace. This stratification implies a legitimacy advantage for the powerholders and outcome dependence (Magee & Galinsky, 2008) for the powerless.

Meanwhile, *they* refer to both external and internal enemies, ranging from international media, activist organizations, and overseas reactionary forces to hostile forces residing in the country and cyber criminals. The media engage in "assignment of praise and blame" (Labov & Waletzky, 1967), attributing positive or negative characteristics to *us* and *them* accordingly.

This section discusses the state's positioning, assignment of rights and duties for involved agentive characters in state-sponsored media discourse.

Development of a Sense of Powerlessness

Legitimation of authority and hierarchy is a causal mechanism that necessitates the engagement of both the powerful and powerless (van der Toorn et al., 2015). According to the authors, from a top-down perspective, this engagement involves political elites and superior classes employing coercion, manipulation, and propaganda through the use of superior resources. Meanwhile, from a bottom-up perspective, the legitimation process requires the motivation of the

powerless to justify, defend, and bolster existing socio-political arrangements. This includes addressing psychological needs for outcome dependence, structure, and the experience of powerlessness. Therefore, powerlessness is considered a key factor in social status, causing disadvantaged groups to be more convinced of the system's legitimacy (van der Toorn et al., 2015). In this process, both the powerful and powerless self-perpetuate and are stereotyped by others. The powerful are often seen as meritoriously successful, while the powerless are viewed, both by themselves and others, as deserving of their plight (Geis, 1993).

The positive association between a sense of powerlessness and system justification has been tested in various socio-political settings, including the legitimation of managerial authorities in workplaces, legitimation of race, class, and gender disparities, legitimation of governmental authority, and general system justification (van der Toorn et al., 2015).

Previous studies also distinguish system legitimation and endorsement among low-status groups in terms of both descriptive (actual achievements of the system) and prescriptive beliefs (ideal goals of the system). Zimmerman and Reyna (2013) found that low-status groups in the U.S. endorse prescriptive beliefs about equality, democracy, and meritocracy more strongly than high-status groups. Similarly, regarding descriptive beliefs, although both groups recognize the system's shortcomings, low-status groups are more inclined to think the system is somewhat better at achieving these goals (Zimmerman & Reyna, 2013). A strong tendency to endorse abstract and definitional beliefs about the system is also found in the Protestant community concerning its work ethics (Levy et al., 2006).

Within the SJT framework, the powerless are often characterized as those worst off in society, possessing limited resources and control over existing reality, failing to speak up on their behalf, tending to endorse negative in-group stereotypes, and using them to rationalize their group's disadvantages (Zimmerman & Reyna, 2013). Consequently, they are dependent on others and uninterested in challenging the status quo (e.g., Jost et al., 2003). Ideological dissonance reduction is an essential mechanism helping the powerless cope with and adapt to inequalities.

Taking the top-down approach, this section aims to examine how the party-state uses media discourse to characterize the powerlessness of laypeople and internet users against the cyber threat backdrop. This includes a careful search for discursive evidence representing cognitive dissonance elements (e.g., the discrepancy between cyber threats and people's capabilities), epistemic components (e.g., people's perception of threats and their consequences, and needs for structure and order), and existential and relational needs to establish a shared reality.

Epistemic Evaluation of Ignorant, Innocent, and Irresponsible Internet Users

State-sponsored media discourse in Vietnam utilizes epistemic evaluation to highlight the awareness and knowledge of internet users concerning technical and functional aspects of cyberspace, as well as their ability to identify and prevent cyber threats. Media outlets frequently stress that "user consciousness plays an important role," noting that "what matters is the perception of users," and cautioning that "users themselves, without the necessary knowledge and skills, may unwittingly abet harmful behaviors in online spaces." However, under the state media's lens, internet users are often victimized as those who easily lose their cautiousness and awareness to cyber scams and crimes. A collocation analysis of terms related to "internet users" reveals a tendency in the media to use passive verbs, such as a*bused, attacked, targeted, affected, victimized*, and *trapped*. Negative adjectives and nouns like *unaware, irresponsible, irresponsibility*, and *ignorance*, as well as negative adverbs such as *unknowingly*, are also prevalent.

The media portray internet users as lacking internet self-efficacy, technical know-how, and awareness of legal violations. Users are described as "easily monitored and manipulated," with "limited awareness, lacking necessary knowledge and experience, and paying little attention to violations of the law related to intellectual property, property ownership, and information about bank accounts or other people's personal property." Consequently, many users "do not know if the information they access is right or wrong, has a scientific basis or not, or affects

others and society." They are portrayed as having a habit of creating and sharing information in an "innocent," somewhat naturalistic way, without being aware of their responsibility for their actions. For example, users are often depicted as "unknowingly sharing web pages that contain illegal gambling or online gambling advertising content, and sharing information that violates the law, is contrary to fine traditions, customs, civilized and progressive lifestyles, etc." Furthermore, the media affirm that "many cases of leaked footage from users' surveillance cameras happened because users did not know how to secure their information." The MPS has stated that personal data leaks occur due to inadequate awareness about protecting data online when sharing it during business activities. Some individuals are even willing to trade their own data for *technological convenience*.

According to the SJT, the contradiction of existential threats to the status quo on one hand, and the portrayal of the powerless, incapable internet users on the other, triggers cognitive dissonance, subsequently motivating people to support and justify existing socio-political arrangements (Jost et al., 2003). In this context, the explanation and justification of the law by the state serve to maintain and justify the potential consequences of the VCSL among citizens. When people are provided with legitimate reasons, they tend to accept the position of power or power differences, in this case, being positioned as powerless; thus, feeling better about being outcome dependent, which helps to gain their compliance (Haines & Jost, 2000). This tendency is even stronger when the issue people are coping with is unfamiliar, such as cybersecurity, and when individual and collective self-interest is low in salience (Jost et al., 2003). Previous studies demonstrate that people with a stronger need for closure and a feeling of dependence on others for access to valued resources have higher needs to reduce uncertainty (epistemic needs), manage threats (existential needs), and uphold a sense of socially shared reality (relational needs) (Jost et al., 2008), as part of an adaptive process of coping and reducing ideological dissonance (van der Toorn et al., 2015).

Moral and Political Assessment of Lay People

In addition to epistemic evaluations that highlight internet users's limited knowledge and ignorance, state-sponsored media in Vietnam also employ moral and political assessments to imply that users deliberately fail to understand regulations under the VCSL. The media use moral standards to delineate right and wrong behaviors through if-clause statements. Responding to public criticism and dissent regarding increased surveillance and investigation of personal information on cyberspace under the VCSL, the media portray dissidents as "lacking good will," possessing "narrow (even dark) will," and exhibiting "irresponsibility towards society and the people."

The media confront dissidents with statements such as: "If you did nothing wrong, no one would take your information for investigation. When the MPS requests one's information for investigation, that person must be a criminal," and "If you deliberately go against or deny those principles (of national sovereignty), it is irresponsible to society and people." Therefore, dissidents are accused of "deliberately hindering the safe and healthy development of Vietnam."

Dissenting comments on the VCSL are deemed "not suitable with the fine customs and traditions of our nation as well as the period of civilized behavior that humanity is aiming for; deliberately distorting the truth, opposing the regime, and going against the people's legitimate interests with hostility."

Regarding negative comments on social events, the media assert: "If you use vulgar language, it is just a violation of morality; but if you deliberately fabricate or spread false information, it is breaking the law." Media outlets warn internet users: "But if you go too far, lack alertness, and feel too emotional, the normal will become abnormal," and address them directly: "If you do not violate the following: Fabricating, defaming, and slandering without personal or organizational evidence, inciting violence on Facebook, fabricating information without precise evidence, propaganda calls to disrupt public order and national security, no one bans the use of social media or prohibits speech."

Patriotism is frequently invoked to assess the moral values of citizens. It is an important value that has accompanied the nation's history and become its distinctive philosophy (Do & Ngo, 2023). The party-state continues to use patriotism as a cornerstone of national policy to encourage internet users to remain vigilant against *peaceful evolution* and *color revolution* instigated by hostile and reactionary forces. On the one hand, the party-state highly praises the patriotism of citizens who express concern about the lawmaking process by making comments and organizing public demonstrations to oppose the VCSL bill. On the other hand, the party-state describes patriotism as a weak point of Vietnamese people who are easily exploited, controlled, and manipulated by opportunists, suggesting that hostile forces incite protests.

Commenting on incidents such as protests in 10 cities and provinces, political leaders imply that participants are morally and politically weak, correcting their wrongful patriotism. Proper patriotism, according to the party-state, is based on an understanding of the law and the nature of social criticism, and should be expressed in a sober, lucid, and responsible manner at the right time and in the right place.

The party-state affirms that in Vietnam, recent events demonstrate that people need to be mobilized and informed about the true nature of freedom, clearly defining the responsibilities and obligations of citizens, knowing right from wrong, and understanding the distinction between building and destroying societal values. This is necessary to protect against those who exploit patriotism and public frustrations to incite unrest. A divided society, characterized by polarized opinions and conflicts, is dangerous in terms of social impact. It can lead to divisions within groups, families, and public spaces, affecting the evaluation of the system, morality, and societal norms. Many people have changed without realizing it, becoming insensitive to human suffering and unable to distinguish right from wrong or healthy from unhealthy behaviors.

An Inescapable Shared Reality

The state media also project a shared reality amidst cybersecurity threats at both national and interpersonal levels to fulfill epistemic and relational needs (Bar-Tal, 2000; Fiske, 2007;

Hardin & Conley, 2001). While Study 1 focuses on analyzing cyber threats that underline existential needs, an interpretation of shared reality in this session examines how state-sponsored media make the constructed reality salient and how it satisfies epistemic and relational needs.

Epistemically, the development of a shared reality provides people with knowledge about themselves and the surrounding world, setting a common ground for collective knowledge and collective recognition of the status quo. This fosters a sense of mutual understanding to satisfy relational needs for affiliation, including needs for social inclusion (Hardin & Higgins, 1996), and reduces cognitive dissonance between existential threats and one's resources. Ideologies, in essence, can serve as "pre-packaged" frameworks of interpretation that facilitate the regulation of interpersonal relationships and the navigation of social and political environments (Jost, Ledgerwood, & Hardin, 2009).

Relationally, a sense of shared reality motivates people to align relationship-relevant attitudes, beliefs, and behaviors towards others in desired or obligatory relationships (Jost, Ledgerwood, & Hardin, 2008) and to distance themselves from undesired or disengaged relationships (Jost et al., 2008). Shared reality cultivates a possibility that shared social norms may reward system-justifying responses and punish system-challenging responses in part to regulate interpersonal relationships (Jost et al., 2008). The motives to align one's attitudes with those held by others (especially ingroup members) play a key role in forming and maintaining stereotypes and other social and political attitudes (Stangor, Sechrist, & Jost, 2001).

To highlight a *dangerous, complicated* cyberspace without cybersecurity, state-sponsored media tend to exaggerate the inescapability and non-exclusion of cyber threats with indefinite phrases such as *no country, nobody, and no one,* using correlative conjunctions like *not only* to emphasize that these threats impact every nation and everybody's daily life. At the national level, cyber disasters are deemed "not only a concern of each individual country, but a global concern," or "not only Vietnam but other countries around the world face challenges from the complexity and difficulty of the internet." Therefore, Vietnam is not the only country that regulates cyber

threats, and the promulgation of the VCSL is adequately justified as "if challenges are not overcome, if challenges cannot be regulated, everyone can be offended." To enhance the credibility of their statements, state-sponsored media rely on external sources to portray an imagination of a world without cybersecurity. State media cited Yeo Siang Tiong, general manager for Southeast Asia at Kaspersky: "we have to accept that cybercriminals will spare no one." A Russian journalist is also cited to talk about *digital dystopia*:

> The 'shutdown' of the cybersecurity industry will open a wide door for criminals to exploit users' data—from financial information and health issues to travel plans and spending. At the same time, fraud in sales transactions is possible as everyone can use someone else's identity to make purchases and even transfer money. Without access control, surveys and e-voting can be rigged. No one has a personal account online, and nothing is private anymore.

At the interpersonal level, a shared reality emphasizes the impotence and inescapability of individuals amidst cyber threats. Against the backdrop of inescapable cyber threats, the state-sponsored media conclude, "No one can cope with cyber threats alone. No one can be safe alone." The use of simple indefinite pronouns in repeated structures makes the shared reality salient, consistent, and less ambiguous. This is also a prominent characteristic of conservative rhetoric and ideology in building system-justifying beliefs (Jost et al., 2003; Lakoff, 2014). Rationalizing the status quo, as opposed to supporting unfamiliar alternatives, is cognitively effortless and enables individuals to maintain emotional consistency across various targets (Eidelman & Crandall, 2012). System-justifying beliefs are particularly attractive to those with (chronic or situationally) heightened relational, existential, and epistemic needs (Jost et al., 2018), as they help individuals satisfy their affiliative drives.

While picturing cyber threats, state media include a wide spectrum from human-related to technique-related aspects with different motives such as financial gains and political objectives targeting both individuals and the party-state. However, when portraying a shared reality, the media focus on personal harms such as personal information theft, online scams and frauds, and exploitation of freedom of speech to slander other people. The adjusted scope of shared reality

serves at least two purposes. First, it makes cyber threats relevant to individuals's lives, implying that everybody can be a victim of cyber criminals. Second, the exclusion of political-related threats marginalizes political perpetrators into *them* who are on the other side of the cybersecurity battle in the homogeneous shared reality of the mass *us*, the victims. The media call a world without cybersecurity solutions a *chaotic world* that "no one would choose to live in" as "we'll be on our own to overcome cyber risks."

Media discourse on the inescapable shared reality not only provides the audience with knowledge but also a commonality of inner states about the world (Echterhoff, Higgins, & Levine, 2009), in this case, a fear of being scammed, hacked, and slandered in cyberspace. After triggering existential threats, the party-state provides a solution for the inescapable shared reality: the enforcement of the VCSL, fostering a sense of outcome dependence and a need for belonging. The law is described as a legal corridor along the socio-economic development process that "leaves no one behind" to demonstrate the human rights and well-being of every citizen. Once the fear of cybercriminals is heightened, shared reality alleviates relational threats, especially when a solution is provided, as individuals will feel included and they are not the only victims. The construction of shared reality consolidates people's worldview, making the constructed reality salient and dismissing competing realities, making social networks homogeneous, satisfying people's identity and social inclusion concerns, and establishing a cognitive repertoire that provides meaning to life experiences (Bar-Tal, 1990; Jost et al., 2018). Thus, system-justifying beliefs produce satisfaction for affiliative needs by making people feel socially connected, subsequently, improving their psychological well-being (Bahamondes et al., 2021).

Relationally, system-justifying ideologies are particularly appealing because they facilitate interpersonal communication and reduce the likelihood of social exclusion. Specifically, because people are generally more motivated to defend the status quo than to challenge it (Jost et al., 2018), system-justifying (vs. system-challenging) beliefs typically enhance relational connections with those around them (e.g., Clark & Kashima, 2007).

Sustaining a shared reality is demonstrated to motivate the endorsement of system-justifying beliefs among those with a growth orientation, driven by an earnest interest in relating to others non-defensively and without fear of negative judgment (Lavigne et al., 2011) and exclusion (Hess & Ledgerwood, 2014). Stern et al., (2014) found that conservatives perceive more in-group consensus precisely because they are more enthusiastically motivated to maintain a shared reality with others.

Political Allegiance and Alienation

The Powerful "We" and Great Leadership of the Party-state

The study 1 discusses how state-sponsored media bolster the VCSL as a timely legal corridor to protect national security, social order, legitimate rights of individuals and organizations with positive adjectives such as *legitimate, lawful, fundamental,* and *comprehensive*. This study, meanwhile, delves into the positioning of *we*, highlighting the party-state leadership as the driving force behind the enactment and enforcement of the VCSL as it is written by the law that "Principles of network security protection are under the leadership of the VCP, the unified management of the State." The state's stance-taking through state-sponsored media discourse is constructed by asserting authority and legitimacy, responding to accusations and criticism, and justifying cybersecurity regulations.

State-sponsored media articulate the party-state's legitimacy through a sustained commitment to building a "State of the people, from the people, for the people" as written in the Constitution 1992. This ideology is continued to be shown firmly in the drafting and implementing of the VCSL that along the process, the party-state has always "listened, respected, and absorbed public opinion in a timely manner," the "Party and State always consider people as both the target and the motivation for the national construction and protection cause, that people are at the center of all policies not only during natural disasters and the pandemic, but in all circumstances, people are always protected and guaranteed in terms of life, assets and living conditions by authorities" and "paying close attention to and directing the work of protecting

network safety and security with many undertakings and policies such as the Strategy on National Defense in Cyberspace, the Law on Cybersecurity..."

The positioning of party-state underscores not only its ideology, goodwill, morality of the party-state but also on the capability to ensure a fair and lawful enforcement of the VCSL: "The Party and State have mechanisms and policies to create conditions for the Fatherland Front and mass organizations to operate effectively and perform the role of social supervision and criticism." And that, "Aware of the importance, benefits and dangers of the internet and social networks, our Party and State have adopted appropriate guidelines and policies to develop the internet and social networks."

Facing allegation of human rights violations, the state reassures that "In Vietnam, the Party and State always respect and guarantee human rights, including citizens' right to freedom of expression," and "Vietnam is a responsible member of the international community, we abide by international law, including Article 19 of the Universal Declaration of Human Rights... The Declaration is still valid, has great human meaning, is always adhered to, inherited and developed by the State of Vietnam in each situation."

> Việt Nam remains consistent that all targets and policies are tailored for people throughout its history, and the Party and the State have made endless efforts to let people fully enjoy human rights and the fundamental rights of citizens.

These propositions are presented in a taken-for-granted manner, implying that they represent indisputable reality (Ton & Hoang, 2023). In the state's discourse, the revolutionary VCP has always been portrayed as an objective inevitability that is selected by history, ruling out other possibilities, trusted by the people, and assigned with the important tasks provided by the Constitution (Vu, 2021). As history has demonstrated, the VCP and its correct leadership are positioned as the cornerstone deciding all the successes of the Vietnamese revolution (Vu, 2021). The industrial revolution 4.0 is no exception.

The leadership of the VCP intertwined with state's leadership, has maintained a steadfast condition for national independence and national survival in state-sponsored media discourse since reunification in 1975 (Mai, 2019). Surferring, surviving, and overcoming from foreign invasion and colonialism throughout history, the protracted struggle for sovereignty and national identity has forged traditional political values with historical and cultural specifics at their core (Fforde & Homutova, 2017). As a result, while nationalism is upheld, the united leadership and the role of the VCP through the U.S. war's victory in 1975, the economic reforms in 1986, and the current socio-economic achievements form the core ideology in communist discourse, enabling the party to sustain its hegemonic position over times (Mai, 2019). The party's leadership continued to be glorified in protecting national sovereignty and security in a non-traditional and sophisticated circumstance, which now includes cyberspace. The party-state considers this as new kind of battlefield, where cybersecurity measures are framed as a national strategy for "Battle of people's security in cyberspace" (Đề án "Thế trận an ninh nhân dân trên không gian mạng). In this battle, leadership of the VCP is positioned as a crucial condition for the effectiveness enforcement of the VCSL: "Firstly, thoroughly grasp the leadership of the Party, the unified management of the State; mobilize the synergy of the political system and the entire people; promote the core role of the specialized force for cybersecurity protection under the Ministry of Public Security assigned by the Government to be the focal point for state management of cyber security."

> History and current reality have proven that: the leadership of our Party and the operation of the State apparatus have led the country to overcome the great storms of the times. Along with that, the Party and State always strive to build a society that is fair, democratic and civilized and puts people at the center of all development efforts.

While the party's leadership is portrayed as undeniable, the importance of national survival is never taken for granted, especially when the party-state defends its shortcomings. The media stress "As long as the country remains, we still have chances to fix what's wrong and become better."

> In fact, no State is absolutely perfect, because the State is an organization formed and developed by people, so is the State. This model will still have shortcomings such as corrupt bureaucracy, moral degradation of a few leading cadres… However, that does not mean that a few "worms" are equated with common shortcomings of a political system.

To reverse the acknowledgment of party-state shortcomings due to *corruption* and *deterioration of political ideology, morality and lifestyle of a part of cadres and party members*, the state-party also claims restored trust on the party leadership among the population "It can be affirmed that the fight against corruption and negativity in recent years has achieved many positive results, regaining the confidence of the majority of the people in the Party's leadership and management."

The discourse of political allegiance on the VCP's leadership to cybersecurity issues mirrors patterns found in other discourse such as anti-corruption. The rosy, optimistic picture painted by the party-state consistently emphasizes the prestige and development of the party and state, and the effective measures and positive outcomes of the party-state's efforts (Ton & Hoang, 2023) within an imagined scenario of "things can be done" (Fforde & Homutova, 2017).

Morality is another pivotal political value that bolsters authority and legitimacy of the VCP. By linking moral values to the great leader Ho Chi Minh's thoughts and tradition of "Uncle Ho' soldiers" as an archetype, the VCP is built on moral standing that aims to earn respect and obedience (Fforde & Homutova, 2017). The national education strategy regarding cyberspace is not diverse from improving an effective education not only in Marxism-Leninism but also Ho Chi Minh's Thoughts. These ideologies have been established as moral standards to differentiate right and wrong views and serve as benchmarks to make "it easier for all classes of people, cadres and parties to recognize the deep-rooted goals of false, hostile views." The close association with President Ho Chi Minh's image is ingrained in political discourse. In a study, Fforde & Homutova (2017) found that interviewees automatically link positive aspects of politics to the glorious past of the Vietnam revolution and the strong moral personality of the President.

By intertwining authority and legitimacy of the united VCP's leadership as an evitable historical selection and nation's revolution, the party-state builds up a protection-obedience equation (Fforde & Homutova, 2017) that fosters the feeling of being protected and the obligations to obey among the populace. The authors argued that the distinction between rule and government was blurred; thus, the political situation in Vietnam is not a "two-way street," where party rule is the powerful and dominant actor, and the population is merely expected to obey, as authority is not granted but rests on fear and deference.

The Positioning of "Them"

As the state frames cybersecurity as a matter of national security and social stability, media discourse expands the concept of *them* beyond geographical and spatial boundaries. *Them* include both internal and external, online and offline enemies, such as hostile and reactionary individuals and organizations, cyber espionage actors, hi-tech criminals or any entities or media outlets opposing the party-state line in general and the VCSL specifically.

In order to quantify state media's description of *them*, the study conducts a collocation analysis of verbs and adjectives that are tagged together with nouns that indicate them.

Them-indicated nouns	Collocations
Hostile and reactionary forces	Nouns: Tricks, opportunists, misinformation, criminals, extremists, conspiracies, accusation, riots, democracy, subversion, poison, immolation, ignorance, weapons, mispresentation, opposition, terrorists, war, cyber attacks, slander, crimes, enemies, dissidents, vigilance, trouble, mastermind Verbs: Spread, fight, distort, oppose, destroy, incite, plotting, exploited, overthrow, sabotage, attack, smash, abet, disgruntled, criticize, carry, provoke, exiled, fabricated, violates Adjectives: Wrong, abroad, anti, dangerous, malicious,

	opportunistic, dysfunctional, baseless, inappropriate, ambiguous, unfriendly, provocative, slanderous, destructive, misleading, ridiculous Adverbs: Deliberatively, fiercely, anonymously, unintentionally, aggressively, continuously
Cyber crimes/cyber espionage/hacker	Nouns: terrorism, attacks, cybercrime, intrusion, dignity, infiltration, appropriation, threat, challenges, malfunction, war, cyberwar, conspiracy, misrepresentation, theft, protests, malware, slander, warfare, risks, infrastructure, consequences, phishing, amateur, victims, raidforums Verbs: causing, combating, infringe, steal, prohibits, hijacking, eliminate, inciting, violate, infiltrate Adjectives: destructive, anti, malicious, professional, unidentified, anonymous, dangerous
Viet Tan, Trieu Dai Viet	Nouns: terrorist, Catholic, reactionary, voatiengviet (Vietnamese VOA), patriot, protest, violence, extremists, Verbs: oppose, sexual, abuse, inflates, exiled, incites, distorting, spread Adjectives: reactionary
"Black" media: BBC, RFA, VOA, RFI	Nouns: enemies, reactionaries, mushrooms, hostile, misinterpretations, fabrications, misunderstandings, curse, bomb, democracy, hackers, crimes Verbs: misrepresented, criticizing, insulting, employ, remove, dominates, spread, attack, emanate, attacked, oppose Adjectives: sensational, negative, biased, destructive, slanderous, abroad, anti

	Adverbs: vaguely, blatantly, mistakenly, widely,

Table 8. Collocate Categorization of *Them*

Since the Renovation in 1986, despite the new foreign policy direction of multidirectionalism, hostile and reactionary forces have remained a prevalent counter-hegemonic discourse with two main themes: the legitimacy of the one-party system and propaganda against peace evolution (Dung & Ho, 2022). "Hostile forces in the country and overseas" have been code words for the Party's rule ever since (Le, 2012). Amidst the wave of law dissent, state media emphasized that "there has never been a time when hostile and reactionary forces had a methodical and detailed plan to distort and eliminate any law like the Law on Cybersecurity." The narrative that demonizes foreign entities, as well as internal enemies, is politically constructed to distance *us* from *them*, triggering nationalism to serve as a form of authoritarian regime maintenance (Babb, 2022) and foster identity-based legitimacy.

The current public discourse reflects counter-narratives between state-led mouthpieces or state actors and civic groups or non-state actors over civil society topics that have existed for many years. In Vietnam's state media discourse, hostile and reactionary forces commonly refer to individuals, groups, and organizations at home and abroad that advocate a liberal approach to civil society, implement *peaceful evolution and color revolution* plots, and take advantage of democracy and human rights to disrupt social order and overthrow the regime. The party's 1991 political report characterizes peaceful evolution as a strategy by hostile forces to promote political pluralism in Vietnam to abolish the party's leadership. This strategy includes spreading depraved and toxic ideology and culture, sending spies and commandos to sabotage the Vietnamese government, and collaborating with reactionary, opportunistic, and disgruntled elements within and outside the country to intensify efforts to overthrow the regime (Hoang, 2021).

These hostile forces are identified with names and faces, including a long list of arrested Vietnamese journalists and activists such as Nguyen Ngoc Nhu Quynh, Nguyen Van Hai,

Nguyen Van Dai, Dinh Nguyen Kha, Nguyen Phuong Uyen, Ta Phong Tan, Dinh Nhat Uy, Truong Minh Tam, and Chu Manh Son. Vietnam-originated democracy parties such as Việt Tân and Tri`ều Đại Việt, along with liberal groups and civil society advocates like the Civil Society Forum, Prisoners of Conscience Association, Association of Women for Human Rights, and Association of Independent Journalists, are also named and shamed. The list is supplemented by international activist organizations such as Amnesty International, Freedom House, Human Rights Watch, and Reporters Without Borders, as well as foreign media outlets like the BBC, RFA, VOA, and RFI. State media discourse frequently attributes negative characteristics to these groups, describing them as evil, dangerous, wicked, regime opponents, or social agitators (A. N. Vu & Le, 2023).

Typically, hostile and reactionary forces are described as:

> Hostile and reactionary forces at home and abroad take advantage of cyberspace to conduct anti-social activities, post false videos, information, and articles, distort the situation of the country, and divide the great unity bloc, ethnic minorities, distort the Party's lines, policies, and laws of the State, smearing and slandering Party and State leaders, inciting people to protest and riot, causing economic, political, national defence, and security instability.

In the context of cybersecurity, the state media has adjusted their framing of hostile forces to maintain relevancy. The current state discourse accuses hostile and reactionary forces of exploiting cyberspace, particularly social networking sites, as a “new front” to perform “old tricks.” State media conclude that these forces oppose the VCSL as they fear “the loss of operational space and failure to implement the measures that are currently being used.”

> A series of reactionary organizations and individuals at home and abroad have set up websites and blogs, and used many Facebook accounts to mold and mix real and fake information, cut pictures, spread rumors, and attract the reader's curiosity. In particular, during important political events in the country, bad elements through Facebook, Zalo, YouTube, etc., post and share a lot of distorted information to lash out, satirize, and distort events taking place throughout the

> country, smearing, fabricating, and discrediting the image of Party and State leaders, leaders of government agencies, causing skepticism among the people, and dividing the great national unity bloc.

The party-state tends to trivialize the motives behind hostile acts, suggesting that individuals only "want to be famous, express personal ego, show off talents, but disregard the law, honor, dignity, and interests of others."

State media blur the distinction among different cyber violations, using hostile acts as an umbrella term to indicate various actions, including fake news dissemination, information and data attacks, software virus dissemination, cyber espionage, and activities inciting regime overthrow.

> Cyber attack activities are diverse and sophisticated. Officials, party members, and the masses need to be alert to the tricks of hostile forces. Currently, they are plotting to attack the websites of the Government, agencies, units, schools, and businesses; fake websites to cheat and steal personal data; malicious code attacks; anonymous attacks with malicious software. Hostile forces will take advantage of personal blogs to entice and incite disgruntled elements, gather forces, and establish transnational opposition organizations, sculpting the party's platform, guidelines, viewpoints, and ideological foundation.

Hostile discourse has been vague and ambiguous in mass media, with interchangeable terms like fake news, trash information, conflicting information, toxic content, erroneous views, and hostile voices that the party-state equates with any content violating traditional media censorship taboos (Nguyen-Thu, 2018). This kind of ambiguity is not uncommon (Kumar, 2021) in both media and law discourse in the country. To Vietnam's leadership, the threat of toxic information is detrimental to its own reputation and the survival and stability of the party and regime in general (Luong, 2018). This ambiguity gives the party-state more flexible terms to regulate and prosecute violations.

Targeting Vietnam-originated democracy groups, the media explicitly state:

> It is a fact that follows the Vietnamese government's declaration that Viet Tan and the Provisional National Government of Vietnam are two terrorist organizations.

These two organizations are framed as the forces behind the opposition to the Special Economic Zone and Cybersecurity Bills, fake news dissemination, and public demonstrations in several cities, especially the vandalism of government offices in Binh Thuan City in June 2018. State media frequently use nationalist tactics to tap into Vietnamese people's deep-seated patriotism and provoke suspicion and hostility against civil society (A. N. Vu & Le, 2023). These organizations are portrayed as "afraid of the light of the sun, hiding in the dark doing evil and cunning things, taking full advantage of social networks, in the name of kindness and patriotism to release a series of articles that distort the truth, confuse black and white, right and wrong."

The media, thus, alert people to not let their patriotism be taken advantage of, "and above all, don't let our people's patriotism be taken advantage of."

On state media, Viet Tan (Việt Nam Cách Tân Cách Mạng Đảng), an overseas Vietnam Reform Party, is framed as a terrorist organization financially funded by the US government and other international donors and Vietnamese living abroad. It is accused of aiming to overthrow the Vietnamese government and the regime in the name of democracy promotion with *peaceful evolution* and *color revolution* plots. However, Viet Tan claims otherwise, presenting itself as a democracy party promoting democracy and human rights in the country through lobbying and non-violent acts (Thayer, 2009). Viet Tan has been a "thorn in the eye" of the Vietnam party-state since its establishment in 1982, and political leaders have purposefully linked all violence and social disorder events in the country to the incitement and support of this organization. The opposition to the VCSL Bill and its consequences on social turbulence in 2018 is no exception. The party-state denies the legitimacy and credibility of hostile individuals and organizations:

> Distorted and slanderous statements that do not come from the voice of the people, do not represent the people, are not by the people and for the people, how can they be called objective, how can the voice of democracy be expressed as what it is?

Targeting international media outlets such as the BBC, RFA, VOA, and RFI, state media describe them as "poisonous mushrooms after the rain."

When portraying these entities, the party-state and its mouthpiece also incorporate emotional factors such as patriotism and nationalist sentiments, great national unity, and anti-Western cultural sentiments to spark wider social support (A. N. Vu & Le, 2023).

Freedom House, Human Rights Watch, and Reporters Without Borders are three major international activist organizations that the state and state media target. In state media discourse, Freedom House is positioned as a *propaganda machine* created by the late President Roosevelt to prepare the American public for America's entry into WWII and later used to conduct propaganda campaigns, advocate for the Marshall Plan and NATO, and propagate against Communism. Similarly, Human Rights Watch is described as "a tool of those who have spent money to operate under the guise of research, monitoring, promoting freedom, democracy, and human rights," using lies to slander and making false statements about the Vietnamese State regarding repression and human rights violations. The state media claim that Freedom House and RSF are funded by U.S. democratic organizations and individuals, serving the *peaceful revolution* and *color revolution* in the country for many years.

> Because of such financial dependence, RSF, Freedom House, HRW... all have the same motive and purpose of action. In fact, RSF operates not in the interests of journalists, who have been denounced in many countries. This organization is also accused of receiving significant support from American billionaire George Soros, who has supported the Solidarnosc union with millions of dollars, and from the National Endowment for Democracy, which receives 90% of its budget from the US national budget and belongs to the US Department of State.

Although U.S.-Vietnam relations have significantly improved politically and economically in the decades following the Doi Moi in 1986, an anti-U.S. sentiment still runs deep among a segment of communist leaders (Pham, 2023). The party-state has always feared that the U.S. will continue supporting the *peaceful revolution* and *color revolution* plots to undermine VCP leadership and regime stability through democratic promotion (Truong Thuy, 2000). Therefore, Vietnam's political leaders tend to link social disorder and incitement with these "foreign elements." Demonstrations in 10 cities and provinces protesting the VCSL bill and the Special Economic Zone are no exception. The media cited General Secretary Nguyen Phu Trong's statement on the incident that "the deep essence is to distort the truth and provoke the people's genuine patriotism to plot other things, having the hands of saboteurs, not excluding foreign elements." According to state-sponsored media discourse, these foreign elements often "seduce and give money to entice people to participate in protests and cause trouble." Organizations and individuals who publicly criticize and organize activities sensitive to the party-state's interests are deemed supported and funded by the U.S. or overseas Vietnamese. High-profile labeled as "bad elements" such as journalists and human rights activists are called "leeches" by the media and are often prevented from meeting with U.S. leaders during trips to Vietnam (Pham, 2023).

The alarmist and combative media discourse reveals the fear among the VCP's hardliners that the U.S. would eventually encourage pro-democracy sentiment in Vietnam and threaten the party's monopoly on power (BBC News, 2023). The link between hostile forces and foreign elements is also propagated by political leaders. Prime Minister Nguyen Tan Dung, on his personal website, called regime critics "phony democrats" and "saboteurs masquerading as democrats" (Nguyen, 2014). It is frequently alleged that these democracy advocates received support from external sources, especially overseas Vietnamese, who oppose the VCP (Nhân Dân, 2014) and rely on contributions from their relatives, friends, and external backers (Công An, 2008). State discourse implies they are betrayers, liars, unpatriotic, and ungrateful for the sacrifices their forebears made to overthrow colonial rule, defeat aggressors, and secure the nation's independence (Công An Nhân Dân, 2009).

Peaceful evolution by hostile forces has remained one of the four major threats to national security or regime security since the mid-term Congress of the VCP in January 1994 (Tung, 2010). However, the VCP's discourse characterizes these as "hidden and increasing dangers that create no-small obstacles to the course of industrialization and modernization of Vietnam and threaten the country's political stability" (Politburo Report, n.d.). This indicates that the VCP views the threats primarily from a domestic perspective, where political stability is of greater concern than national security (Tung, 2010). In Vietnam, politics is often treated not as "everyday" or "petty" politics (i.e., politics with a small p) but as anything that the VCP perceives as a challenge to its monopoly of power (politics with a big P), including regime change, calls for multi-partyism or pluralism, or independent labor unions (N. A. Vu, 2017).

Disalignment With "Them"

State-sponsored media primarily use epistemic evaluation to enhance the credibility of their statement on *them*, presenting their assertions as factual and reflective of reality (Langacker 2009, 173). Rather than relying on judgment and subjectivity, state media invoke the "past transgressions" and "past actions" (Badarneh, 2020) of alleged hostile and reactionary forces to undermine their current credibility and implicitly indicate their persistent accusations against the party-state. In addition, state media employ epistemic stance-taking by displaying familiarity with *them* and their old tricks, thus reinforcing their competent identity (Johnstone, 2016). This familiarity is affirmed with evidentiality markers indicating a high degree of certainty (Nuyts 2001, 22), such as "as usual," "it is not difficult to recognize," "clearly," and "obviously," to suggest that the the existing knowledge about them is certainly supported by evidence (Cappeli 2007).

For example, regarding foreign media's reportage on the incident involving Viet Tan, a self-claimed democracy party, and Reporters Without Borders lobbying some U.S. lawmakers to oppose the VCSL draft in 2018, state-sponsored media commented, "As usual, some foreign media outlets like VOA, BBC, and RFI have published articles with a "scaremongering" and

“overbearing” tone, exaggerating information” (Cam Ranh Portal, 2018). Or, “It is not difficult to recognize those false and out of place claims of foreign news agencies, press and domestic political opportunists.” Or “Obviously, the truth of those of RSF, Freedom House, HRW... has been revealed for a long time, the same guise, tricks of fraud, deception and slander as before, although today's trend has changed a lot.” Or “Criticizing and condemning the Party and State of Vietnam on democracy and human rights, this is nothing new.”

The use of epistemic evaluation exerts control on the audience’s acceptance of the perceived reality (Biber et al., 2021) and the status quo regarding the existence of these hostile forces. State media discourse on *them* represents a kind of stereotype about them that does not originate from the “kernel of truth” but rather derived from prevailing systems of existing social arrangements (Jost & Banaji, 1994). Previous legal tools, including the Penal Code, especially Articles 79, 88, and 258, are also used to tackle hostile acts. These legal tools provide the state with a broad mandate to define and criminalize a wide range of activities as hostile acts. By leveraging these laws, the state can prosecute activists, journalists, and other dissenting voices, effectively curbing opposition and maintaining control over the political landscape. Moreover, the state's use of these legal tools is often supported by media narratives that depict those targeted by the laws as threats to national security and social stability. This creates a feedback loop where legal actions against individuals and groups reinforce the media's portrayal of them as hostile forces, which in turn justifies further legal actions. This synergy between legal measures and media discourse ensures that the state's narrative remains dominant and unchallenged.

State media reject the standpoints of hostile forces on freedom of speech issues:

> It can be easily identified and statistically shown that hostile elements and political opportunists are always looking for ways to create the so-called "free speech" in a childish, narrow, and full of grudges with evil schemes.

> The hostile forces have a one-sided view that in Vietnam social networks are suppressed and social networks do not have freedom of information, social network users are not allowed to express their opinions and thoughts... This is completely fabricated and untrue information because our Party and State have always consistently advocated and maintained the policy of respecting and protecting basic human freedoms, including the right to self-determination.

Furthermore, besides affective, attitudinal, and epistemic evaluation, the media also use interactional (dis)alignment to express agonistic views of dissidents and critiques from international media and human rights organizations. The state media not only disalign with these organizations by rejecting their accusations but also reproach, blame, confront, challenge their statements, and question their accuracy, authority, and legality, as well as their motives to make such conclusions. These discursive responses serve as a general "social defence" strategy against the formation of negative self- or in-group impressions (Van Dijk, 1992: 92). By challenging these claims, the state not only positions itself as a victim but implicitly indicates the mentioned organization as deceptive. The construction of victimhood involves positive self-positioning and negative other positioning (Harre´and Van Langenhove, 1991, 1999). Meanwhile, questioning the credibility of these claims implies a hidden agenda by these organizations, thereby, undermining the validity of their accusations.

The distinction between *us* and *them* in cybersecurity discourse has become considerably more prevalent after the 9/11 incident to refer to terrorist attacks on, particularly, Western society, values, and morals (Bowman-Grieve, 2015). The contrast between *us here good* and *they there bad* or the legitimization of us and delegitimation of them is common in political discourse. This construction or reliance on a specific ideological narrative to increase a regime's legitimacy often goes hand in hand with the demonization of foreign entities by labeling these threats (Babb, 2022). One needs to establish legitimacy or "right to be obeyed" through positive-self (e.g., self-praise, self-justification, self-explanation) and negative-other (e.g., blaming, scape-goating, marginalizing, denying) presentation as a source of authority, reason, vision, and sanity (Chilton, 2004). Compared to other types of authoritarian regimes, single-party regimes are the most

active ones in using tactics to legitimize their rule, prop themselves up, and delegitimize their rivals (Dukalskis & Patane, 2019). Targeting hostile forces and black media, state-sponsored media use accusatory discourse to alter the audience's attitudes toward the accused and create new negative attitudes about them (Benoit and Glantz, 2017).

Marginalization of "Black Sheep" Among "Us"

Through national media discourse, the party-state not only alienates hostile and reactionary forces from *us* but also sets moral standards to distinguish and marginalize "black sheep" among us. While VCSL is defined as a legal corridor to protect national security, network security, and legitimate rights of individuals and organizations, the media distinguish "ordinary users" from the others primarily based on the user's obligations to protect national security and interests.

> Ordinary network users are well aware of and avoid acts of violating the law on national security, social order and safety (related to the posting and distribution of anti-State information, accepting the ruling role of the VCP, providing offensive information to the Party and State's leaders, abusing democratic freedoms to infringe upon the interests of the State and the legitimate rights and interests of the organization, individual…). However, in fact, some people, due to ignorance and irresponsibility, have been "trapped" by bad actors when sharing fabricated information hidden in information that "seems true" or mixing events, real characters with fake news, or real news but with slanderous political commentary (especially on YouTube).

State media emphasize that *laws, regulations, and codes of conduct on social networks only work when users are wise and know how to discern fraudulent content*. When international media outlets criticized the VCSL on their Facebook posts, the government demanded Facebook restrict and suspend this content and deployed Force 47 to report these posts as violating community standards. State-sponsored media stressed, "Only patriotic Vietnamese Facebook-ers would report to the Facebook network operator about the act of spreading information that incites violence posted on these websites."

A country with nearly 40 million individual accounts participating in social networks, but only a very small minority opposes, with impure motives.

And that,

Hostile and reactionary forces oppose the VCSL in order to obstruct and cause panic and suspicion among the people; some objections due to lack of understanding of cyberspace, not understanding the law, even some people who have never read this law also follow other people's objections.

Similarly, to further separate *them* from *us*, the state media assert:

For the State and our people, the promulgation and strict implementation of the VCSL is one of the important guarantees and an effective measure to ensure human rights, legitimate rights and interests of citizens. help prevent and handle illegal acts in cyberspace, contributing to protecting national security and maintaining social order and safety. For them (hostile and reactionary forces), the VCSL deprives them of important weapons that they can use to accomplish their goals of subverting, overthrowing, and transforming our regime into an alien "democracy" and "human rights" path.

State media further dismiss distorted and slanderous statements, asserting that they “do not come from the voice of the people, do not represent the people, are not by the people and for the people.” They emphasize that “perhaps among us, no one supports criminals thoroughly taking advantage of the Internet's utilities, especially social networks, to conduct activities that infringe on security and order, causing instability in society.”

Regarding the incident where a dissident raised an "anti-VCSL" slogan at a live football match of the Vietnamese team at the AFF Cup on national TV in 2018, state media condemned it as "lost, shameless," and dismissed it as just a "single image."

Although the party-state acknowledges some shortcomings in governance, including corruption and moral degradation among some party members, it marginalizes these individuals

as "a few worms" that do not represent the common phenomenon. This narrative aims to preserve the overall image of the party and state while isolating and condemning those who dissent or fail to meet the established moral standards.

Rights and Obligations of Relevant Parties

Rights and Obligations of Citizens

The presentations of the rights and obligations of citizens, as well as relevant stakeholders including authorities, aims to address people's uncertainty and fear of cyber threats while setting the stage for the party-state to lead the country in overcoming and winning the cyber battle. This approach, on the one hand, satisfies the epistemic needs of lay people by reducing uncertainty and ambiguity (Jost, 2019) regarding cyber disasters depicted by the state. On the other hand, it provides the state's justification for citizen's institutionalized obligations, balancing these with their rights. An analysis of state discourse on rights and obligations, moreover, helps to indicate power distance and political position of citizens in the one-way relationship with the authorities, defining the space where citizens can or cannot compromise their rights with their obligations.

Citizens, particularly internet users, are placed in the heart of the VCSL as the primary beneficiaries and targets of the law, which serves as the state's motivation for national construction and protection. In state media's discourse, however, they are positioned as subordinates who must comply fully with both legal responsibilities and socio-moral commitments. The VCSL establishes a legal framework within which internet users must operate, mandating compliance with regulations designed to protect national security and public order. Decree 72 complements this by outlining the management and use of internet services, thereby, emphasizing the necessity of responsible usage. The government's stance is clear, ignorance of the law is not a valid defence. Users are required to educate themselves about these regulations and ensure their behavior conforms to the established legal standards.

Obligations of internet users and citizens are frequently accompanied by a combination of modal verb (i.e., *must, should*) and upscaling adverbs (i.e., *strictly, completely, fully, definitely, firmly, immediately*), or adverbs of frequency (i.e., *always)*. For example, citizens are required to "must always comply with Constitution and the law," "must always be alert of information posted," "must ask the authorities to protect," "must be accompanied by disciplines and law," "must be aware of the use of the network," "must be calm," "must be careful," "must be responsible for their actions and statements on cyberspace," "must compensate [if violate the law and case social damage]," "must immediately report to the relevant authorities," "must clearly know and properly understand that the law allows doing," and so on.

The party-state delineates the boundaries within which individuals and organizations can operate, marking the line between permissible and impermissible actions. This framing is particularly evident in discussions of human rights and freedom of expression. While the state acknowledges these rights, it places significant limitations on them to ensure they do not conflict with national security and public order. The government's reassurance that freedom of expression is protected under the Constitution, laws, and international agreements is tempered by the caveat that this freedom is not absolute. The legal framework is designed to prevent the abuse of speech, which could infringe upon national interests and the legitimate rights of others. This approach underscores that freedom of speech must be exercised responsibly and within the legal confines, prioritizing the common good over individual liberties (Vu & Ha, 2021).

> Obviously, in any political regime, there can be no absolute freedom of speech. Countries strictly handle acts of abusing freedom of speech; promoting freedom of speech must be for the common good, not the absolutization of individual freedom, not taking advantage of freedom of speech to write, speak, or distort with bad intentions, regardless of morality and law. Freedom is a human right, but it is not an arbitrary, anarchic freedom. It is only guaranteed when people properly perceive the objective law and act in accordance with the law agreements and agreements on the freedom of the collective, community, and society.

When exercising citizen's rights, people are reminded to be aware of its limit specified in anti-party-state acts such as "people can completely express their opinions and views on cyberspace but they must not take advantage of that to propagate against the State of the Socialist Republic of Vietnam; inciting riots, disrupting security and disrupting public order; humiliate, slander; infringing upon the order of economic management…"

The government's advocacy for a populace capable of discerning credible information from falsehoods is essential for mitigating the spread of misinformation and disinformation. Users are encouraged to critically analyze information, question its sources, and verify its authenticity before sharing it. This responsibility transcends personal obligation and becomes a civic duty, as unchecked misinformation can erode societal trust and disrupt social harmony.

Patriotism remains a core value of Vietnamese national identity and is actively promoted as a civic duty in the digital age. The government's use of patriotic rhetoric aims to foster a sense of national unity and vigilance among internet users. This is particularly pertinent in countering *peaceful evolution* and *color revolutions* propagated by hostile forces (Do & Ngo, 2023). The state defines proper patriotism as a lawful and rational expression of national pride. Internet users are encouraged to support the nation's socio-economic development goals and protect its positive image. This includes being cautious about sharing content that could harm national interests or be exploited by adversarial entities to destabilize the country.

Ethical online behavior is another critical obligation highlighted by the government. The importance of a civilized online culture is emphasized, where users are expected to respect the Code of Conduct on social networks. This involves refraining from posting or sharing unverified or harmful information, which could have negative consequences for society or national security. Users are encouraged to contribute positively to the online community by posting content that is truthful and constructive. The broader impact of online actions is a significant consideration, as irresponsible behavior can lead to substantial societal consequences. By promoting a culture of

ethical online behavior, the government aims to build a more resilient and cohesive digital society.

Overall, the obligations of internet users, as outlined by the Vietnamese government, are extensive and deeply integrated with the broader objectives of national security, social stability, and moral-cultural preservation. Compliance with legal regulations, fostering digital literacy, embracing patriotic values, and practicing ethical online behavior are seen as essential components for a safer and more unified digital environment. These obligations are not solely individual responsibilities but are crucial to the collective well-being, political stability and social order. The assignment of these duties and obligations on citizens serves to restrict and shape their modes of action (Badarneh & Migdadi, 2018).

Although the party-state emphasizes its people's rights and asserts that citizens are central to the law and the policy-making process, the government's propaganda implicitly suggests a lack of encouragement for political participation in terms of several perspectives.

First, the legal and institutional framework of the VCSL is designed to consolidate the VCP's control with the MPS as the main force for law implementation. Consequently, political activities outside the VCP's structures are largely prohibited, meanwhile, peaceful dissident activities and demonstrations in public places are implicitly discouraged. More critically, a regulation on broad and vague definition of “wrongful” statements including insults to individuals, organizations, political leaders, and the party-state is also applied to restrict public criticism. Violations are handled by the MPS.

Second, the political culture in Vietnam discourages active citizen engagement in politics. The state promotes a form of civic participation that aligns with the party's goals, such as community service and local governance involvement but discourages activism that seeks to challenge the status quo. Public discourse is managed through state-controlled media, which emphasizes national unity and socio-economic development while minimizing coverage of political dissent.

Moreover, the education system and public messaging in Vietnam reinforce the narrative of political stability and economic growth as paramount, often sidelining discussions about political freedoms, citizen participation, and civic society. Citizens as well as party members and cadres are encouraged to equip themselves strongly with Marxist-Leninist Theory and Ho Chi Minh Thought to behave lawfully and morally in cyberspace. This has created a political environment where many citizens may be disinterested or feel powerless to engage in politics beyond the sanctioned forms of participation.

The state media discourse on the rights and obligations of internet users and citizens, in general, employs a combination of hard power to enforce legal obligations and soft power to invoke moral commitment and patriotism, revealing power constraints in the country. However, the assignment of rights and obligations also serves a subjective side as it fosters a sense of social belonging, strengthens national and multidimensional identity, and makes people perceive themselves as members with efficacy in social and political entities (Dahlgren, 2005).

Rights and Obligations of Party-state

In parallel with the assignment of rights and obligations to the populace, a strong domain of party-state's obligations is also presented. The government emphasizes the importance of having a "centralized, transparent, synchronous, unified leadership and direction, and a clear assignment of responsibilities among agencies" to ensure national sovereignty protection and network safety. The party-state, encompassing both governmental authorities and specialized agencies, occupies a dual role in Vietnam's cybersecurity landscape. On one end, it serves as the protector against cyber attacks and hostile forces. On the other, it acts as a servant to the people, committed to respecting and absorbing public opinion, guaranteeing human rights, and developing policies that foster a fair, democratic, and civilized society. The party-state's discourse often emphasizes proactive and attentive actions such as "respect, listen and absorb public opinion in a timely manner," and "respect and guarantee human rights." This rhetoric

serves to reassure the public of their central role in governance while implicitly indicating the government's overarching control.

Regarding legislative obligations, government agencies are encouraged to actively review and perfect the legal system related to information security, improving the capacity, effectiveness, responsibility, and coordination of information management. Serving ideological duties, the Fatherland Front plays a crucial role in uniting and mobilizing the populace, fostering patriotic initiatives, and enhancing national unity. Traditionally, the Fatherland Front is positioned as a vital body in promoting democracy, strengthening social consensus, supervising and critiquing societal issues, and contributing to party-state development as well as international relations. Meanwhile, other bodies, like the national press, are assigned to support lawmaking by safeguarding public interests and freedoms and overseeing policy implementation, contributing to exposing and combating corruption, and providing timely and transparent information on national affairs. However, none of these agencies wields as much power as that of enforcement bodies.

While each government body has its authority and function to serve the citizens, the MND and the MPS, in particular, are granted significant power under the law. The Cyber Command under operation of the MND is defined as "plays a pivotal role in ensuring national cyber security and safety, fighting against high-tech crime and peaceful evolution in cyberspace." Meanwhile, article 19, 20, 21, 26 in the VCSL empower and give the MPS the authority to demand access to any organization or company's data system for investigations where there is a perceived threat to national security and public safety. Chapter 3 of the VCSL stipulates that the MPS is responsible for protecting national security and social order in cyberspace. The MPS is also the state management agency and the focal point for the certification and licensing of national cybersecurity standards and regulations. The MSP is frequently assigned with strong nouns and verbs such as *prevention, protection, cooperation, control, stipulate, coordinate*, *investigate,* and positively duty-related adjectives such as *professional, specialized, functional, and proactive*. A collocation analysis shows that referent

objects within the duty scope of the MSP include *government, safety, agencies, organizations, data, business,* and *individuals* .

The MPS is tasked with developing draft national standards on cybersecurity and proposing, appraising, and promulgating national technical regulations for information systems crucial to national security. To date, authorities have summoned individuals, forced the removal of false information, and obtained commitments to prevent repeat offences. Both the MND and the MPS proactively detect, fight, prevent, and strictly handle those who exploit the internet and social networks to violate the law.

> The MPS has had many active activities in detecting, investigating and handling violations of the law on cyber security. In 2019, the MPS has strengthened measures to clarify new methods and tricks of criminals using high technology in online transactions and electronic payment activities, and dismantled many criminal lines of gambling and betting on football via the internet.

The centralization of cybersecurity power within the MPS is a result of a regulation heavily focused on national security and an exaggerated emphasis on existential threats to the regime, and it has a significant impact on freedom of expression. The extensive powers granted to the MPS have raised concerns about the suppression of free speech and increased censorship. Critics argue that these powers can be used to silence dissent and control public opinion, thereby stifling democratic discourse and limiting political freedoms. Additionally, the requirement for data localization and the accessibility of personal data to the MPS pose significant privacy concerns. Individuals' personal and sensitive information can be easily accessed by the authorities, leading to fears of surveillance and potential misuse of data. The power centralization into the MPS's hands underpins an even broader and more robust legal framework, advanced operational capabilities, and stringent enforcement actions.

6.4. Reflection on SJT

The SJT posits that people have a psychological need to perceive existing social, economic, and political systems as just, legitimate, and necessary, even if these systems disadvantage them (Jost & Banaji, 1994). This need is particularly pronounced when individuals feel powerless or vulnerable. In the context of the VCSL, the portrayal of citizens as powerless against the powerful leadership of the party-state plays a crucial role in fostering support for the law and the ruling regime.

Interpreting the study findings under the lens of the STJ, individuals experiencing powerlessness often seek cognitive closure, which is the desire for a firm answer to a question and an aversion to ambiguity and uncertainty (Kruglanski, 2004). The portrayal of cyber threats as pervasive and complex creates a sense of chaos and insecurity, even a sense of death. In this scenario, the VCSL is presented as a clear, definitive solution that promises protection and order. The need for cognitive closure can help to increase the likelihood of individuals to accept the VCSL because it provides a sense of certainty and predictability in an otherwise uncertain environment. This aligns with their psychological need projected by the SJT to reduce the discomfort associated with ambiguity and complexity.

Moreover, the perception of existential threats, such as cyber attacks, heightens anxiety among powerless individuals. This anxiety creates a strong foundation for system justification as a coping mechanism (Jost et al., 2007). When faced with threats they feel incapable of addressing, individuals are more likely to endorse measures that promise to mitigate these threats, even if these measures are imposed at the cost of their fundamental rights and well-being. The VCSL, framed as a protective measure against cyber threats, taps into this anxiety, and can act as a trigger making individuals more inclined to support it.

Powerless individuals often develop a heightened sense of dependency on those perceived as capable of providing security and stability (Kay et al., 2009). The state's portrayal of itself as the sole protector against cyber threats reinforces this dependency mechanism. By

emphasizing the complexity of cyber threats and the specialized knowledge required to combat them, the state positions itself as indispensable. This dependency aims to foster a belief in the legitimacy and necessity of the VCSL, as state media primed people's well-being to be directly tied to enforcement of such laws. This reliance on authority helps to maintain the status quo by validating the state's control and intervention in digital spaces.

In addition, SJT posits that system justification serves to bolster self-esteem, particularly among individuals who feel marginalized or powerless (Jost & Hunyady, 2005). By aligning themselves with a powerful and protective state, powerless individuals can derive a sense of worth and security. Therefore, the media framing of shared reality can facilitate a sense of belonging, allowing people to feel part of a collective effort to safeguard national security, and subsequently might enhance their self-esteem. This psychological mechanism might benefit the system as it makes people more likely to justify and support the existing system as well as compliance with the law.

Furthermore, the repeated frames of the VCSL as essential for protection against cyber threats and strong disalignment with dissenting voices can lead to the internalization of these narratives, especially among powerless audiences (Bandura, 2001). In a closed and highly censored media environment like Vietnam, powerless individuals, lacking alternative sources of information or the ability to critically evaluate the state's claims, are more likely to internalize these narratives and accept the VCSL as necessary and justified. This internalization process ensures that the state's perspective becomes the dominant lens through which individuals interpret their social and political environment.

Additionally, powerless individuals often seek belonging and identity within the dominant social group. The state's portrayal of supporters of the VCSL as patriotic and loyal citizens can fosters a sense of in-group favoritism (Tajfel & Turner, 1986). By supporting the VCSL, individuals align themselves with the in-group, enhancing their social identity and acceptance within the community. This social alignment further reinforces their justification of

the law and the ruling regime. The desire to be seen as part of the loyal and patriotic majority encourages individuals to conform to state narratives and policies, even if they have reservations.

Moreover, cognitive dissonance arises when individuals experience a conflict between their beliefs or with actions. The state media projected different attributing scenarios for the dissonance including the powerlessness of lay people versus cascading consequences of cyber attacks, and the repressive nature of the VCSL versus its warrant of security. By fostering a strong sense of system legitimacy and outcome dependence, state media can influence the tendency of psychological adjustment that helps people to maintain a coherent worldview that aligns with their actions and perceived interests. As a consequence, if people see the VCSL in a positive light, they can reconcile any internal conflicts and continue to support the state's measures without feeling hypocritical.

Another significant factor in the justification of the VCSL is the state's portrayal of hostile forces as existential threats. The media depict these hostile forces as not only opposing the VCSL but also undermining national security, social stability, and public morality. This portrayal taps into not just the primal fear of external threats but also group identity, which in turn justifies stringent security measures. By framing opposition groups as dangerous and morally corrupt, the state creates a dichotomy between the patriotic in-group and the treacherous out-group. This alienation of hostile forces serves to marginalize dissenting voices and rally public support around the VCSL. The perceived threat from these forces makes the public more amenable to accepting restrictive laws as necessary protections.

In short, as posited by the SJT, the psychological factors for system justification deeply rooted in human needs for security, certainty, self-esteem, social identity, and cognitive consistency. By capturing this mechanism and portraying citizens as vulnerable and the state as a necessary protector, the Vietnamese party-state can influence people perception and leverage these psychological dynamics to foster a likelihood of compliance and support for the VCSL. In a broader context, understanding these psychological underpinnings provides valuable insights

into the mechanisms of system justification and the ways in which authoritarian regimes maintain legitimacy and control over their populations.

Chapter 7. System Justification Strategies of the VCSL on State-sponsored Media

7.1. Research Objectives and Research Design

This study analyzes media discourse focusing on the system justification strategies employed by the state and mainstream media to legitimize cybersecurity law and its controversial regulations. By leveraging the SJT, the research investigates five key ideological strategies: authorization, rationalization, moralization, denial of system problems, and stereotyping or the delegitimation of opposing elements. Through a comprehensive examination of both text and context, this study aims to reveal latent ideologies and justification strategies employed by state and media actors in the rationalization process.

This study uses mixed methods with quantitative content analysis and critical discourse analysis. A manual content analysis is an essential step to identify, sort, and categorize themes of cyber-security discourse and media's justifications for the VCSL promulgation and enforcement. Justification strategies, according to the SJT, such as rationalization, legitimation, denials of system problems, and complementary stereotypes are used as main categories. While content analysis only provides a descriptive analysis of data, the CDA is used as an elaborative and parallel step with content analysis to comprehend ideology, power, and hegemony (Fairclough, 2010) of the party-state along with the enforcement of the new law and regulations.

7.2. Research Methods and Materials

This study uses news articles in the "National News" corpus as analysis units.

Content Analysis

For quantitative content analysis, the author first closely read through all articles to initially spot the common strategies of media's justifications on the VCSL. While maintaining an open coding tactic, these patterns were primarily identified based on postulate III of the SJT, which are: direct endorsement of certain ideologies, the legitimation of institutions and

authorities, denial or minimization of system problems or shortcomings, complementary stereotyping, and rationalization. Second, after having the preliminary coding scheme, the author randomly selected and coded 85 articles (20% of the sample) for pilot purposes. One article could mention 1 or more than 1 of these justifications. During this step, a final coding scheme was confirmed and refined by removing minor categories and combining relevant ones. There are five major justification strategies with 18 categories used for the final coding.

The first strategy is *"Authorization"* which covers both impersonal authority, personal or positional-based authority, and authority of conformity. The first category is "impersonal authority" with articles that make the law references to legal or documentary sources such as Constitutions, Penal Code, or international agreements. The second category is "personal authority" with articles making references to the elites or experts. The third category, "law conformity/consensus," was coded if articles mentioned that the law aligns with the *1992 Constitutions, international binding, agreements, international regulations*, *bilateral or multilateral commitments*, and that the law is a *common trend* or n*ot one of a kind*. In addition, articles stated that the law received a *high approval rate* at the Assembly, *high consensus among citizens*, and *positive feedback* from *national* and *international public* was also coded under this category.

The second strategy covers the media's *"Rationalization"* of the VCSL's promulgation in fighting against cyber threats targeting 4 main endangered value categories and two main benefits of the law. The first category under this strategy is "national security." Articles fall under this category if mentioned endangered values are *ideology, internal affairs, regime security, national unity, sovereignty, state secrets, state policies*, *national defence*, and *party lines*. The second category is "information security" with articles mentioned about *infrastructure, network security, personal data protection, network safety, infrastructure technology*, or any types of *hi-tech criminals*. The third category mentioned legitimate and lawful "rights and interests of individuals and organizations." These rights and interests include *human rights, human development, children protection, rights to freedom of speech, rights to*

privacy, social media use, economic interests, and any acts that harm those rights of individuals and organizations. The forth category in this strategy is "social order and stability." Articles were coded if they mentioned *social safety, political stability, peace, religious grace*, and any acts that disturb *social order*. The fifth category, "Legal corridor improvement" was coded if the articles said the law is to *complete, build,* or *create standards* for the current incomplete legal corridor. In other words, this category consists of articles that indicate keywords such as *institutional improvement*, *law improvement, system development, and system sustainability*. The last category in this strategy is "economic development" with articles mentioning benefits such as *business environment improvement, digital transformation, economic infrastructure*, and *foreign investment enhancement*.

The third strategy *"Moralization"* was coded into two strategies, which are "moral values" and "cultural standards" or "fine customs" of the country.

The forth strategy is *"Denial of system problems"* with 5 categories. "Power abuse" was coded if articles denied that by implementing the law, there is no power abuse; and any persons or authorities violating citizens and enterprises' rights will be punished. "Control of personal data" was coded if articles rejected accusations that the law enhances the government's surveillance and exploitation of cyber or personal data. "Violation of human rights" was coded if articles persisted that the law does not infringe human rights that include freedom of speech, freedom of expression, freedom of press rights to freedom and democracy. Articles that claimed that the law was only to set boundaries of such rights were also coded under this category. "Business barriers creation" was coded if articles claimed that the law does not generate sub-license or hinder business operations in the country. "Violation of international agreements" was coded if articles denied accusation that the law violates any international agreements such as GATT 1994, GATS, TRIPS, CPTPP or regulations on data storage.

The last strategy, *"Stereotyping/delegitimation"* has two categories. "Hostile and reactionary forces" was coded if articles mentioned the existence of *hostile and reactionary*

forces, *opportunistic elements*, or *dissidents* who have been always trying to *overthrow* the regime, *disturb* social order, and *distort* state-party lines. "Foreign media/organizations" was coded if articles blamed and shamed uncooperative organizations such as overseas groups who steal and sell personal data; unfriendly foreign telecommunication companies that do not cooperate with the government timely; black media that say unfavorable lines towards the state-party, and international human rights groups (i.e., Human Rights Watch, Reporters Without Borders) that criticized and downgraded human rights situation in Vietnam.

After having a finalized coding scheme, the author and another colleague separately conducted the coding on the same random sample of 10% of total articles (n= 42). Inter-coder reliability was then calculated. The mean coefficient of strategy "authorization was .68, "rationalization" was .65, "moralization" was .75, "denial of system problems" was .79, and "complementary stereotypes" was .70. There was no category that had reliability under .65. The two researchers also discussed and found agreement on disputable cases before coding the remaining articles in the corpus.

Critical Discourse Analysis

CDA serves as an essential methodological tool in this study, providing a comprehensive framework for uncovering the complex ways in which language is employed to construct social realities, maintain power dynamics, and reinforce the ruling regime's legitimacy. CDA allows for a systematic examination of how state-sponsored media embed ideological constructs within their narratives. By deconstructing the language used in media texts, CDA reveals how the VCSL is portrayed not merely as a legislative measure but as an essential and justified tool for maintaining national security and political stability. This aligns with Fairclough's (1995) assertion that media texts are both modes of representation and interaction, constructing social identities and relationships.

While Study 1 and Study 2 focus more on contextualization, emphasizing the importance of situating discourse within its broader socio-political context, this study delves into revealing

how ideologies are constructed into different narratives used by the party-state to rationalize, bolster, and defend the legitimacy of the law and the regime in general, and subsequently, reproduce power and dominance (van Dijk, 1993). Rooted in legitimation categories proposed by Van Leeuwen (1996, 2007, 2008) and combined with guidelines from the SJT, this study addresses primary justification strategies used to legitimize the VCSL, including authorization, rationalization, moralization, denials of system shortcomings, and stereotyping/delegitimization.

Each of these strategies is considered within the broader historical context and ongoing control of the VCP, and analyzed through the interplay of lexical choices, power, and ideologies. These strategies are not completely exhaustive but are interconnected to supplement and strengthen each other. For instance, rationalization strategy narratives highlight the benefits of the law for national security and public order, presenting it as a logical and necessary solution to specific problems, such as cyber threats. Moralization strategy, on the other hand, frames compliance with the law as a moral duty, aligning the VCSL with societal values and norms. This dual approach strengthens the public's acceptance of the law by appealing to both reason and morality (Wodak & Meyer, 2009).

This study synthesizes findings and arguments from the two previous studies, extending beyond lexical analysis to develop a broader ideological construct and social practice of the ruling regime. By examining these justification strategies, CDA sheds light on how state-sponsored media constructs narratives that justify the VCSL and reinforce the ruling regime's legitimacy. The analysis demonstrates the complex ways in which language is used to support system justification, mitigate opposition, and maintain social order. Through CDA, the study provides a theoretical and empirical understanding of the mechanisms that underpin media discourse in authoritarian contexts.

7.3. Findings and Discussion

Content Analysis

Classification of justification strategies and categories are summarized in Table 9.

	Number of instances	Percentage
Authorization		
Impersonal authority	22	5.2%
Personal authority	10	2.4%
Authority of conformity	76	18.1%
Rationalization		
National security	112	26.6%
Information security	90	21.4%
Rights and interests of individuals and organizations	101	24.0%
Social order & stability	48	11.4%
Legal corridor development	45	10.7%
Economic development	35	8.3%
Moralization/Moral legitimation		
Moral values	15	3.6%
Cultural standards/custom	17	4.0%
Denial of system problem		
Power abuse	32	7.6%
Control of personal data	20	4.8%
Violation of freedom of expression	75	17.8%
Creation of business barriers	38	9.0%
Violation of international agreements	19	4.5%
Stereotying/Delegitimization		
Hostile and reactionary forces	75	17.8%
Foreign media/organizations	51	12.1%

Table 9. Classification and Distribution of Justification Strategies

For comparison purposes, instances of justification strategies are grouped into three different periods. The first period is from 2017 to 2018 when state-sponsored media started to propagate the need for cyber security in the country and introduce the draft law at the 14th Assembly. The second period is from 2019 to 2020 when the law takes effect in early 2019. The

third period is from 2021 to 2022. This timeline was chosen as after the VCSL enforcement in 2019, the government continued to issue supplementary directives and decrees such as the social media Code of Conduct in June 2021, 70/2021/NĐ-CP in September 2021 providing supplementary regulations on cross-border advertising, and Decree 53/2022/NĐ-CP in June 2022 providing more details on some articles in the VCSL. Findings of justification strategies and categories are summarized in Table 9.

The results from one-way ANOVA tests show that there as a statistically significant difference between phases in terms of the numbers of news articles published on state media ($F(2,150) = 151$; $p < .00$). A Bonferroni post-hoc test indicates that the there was significantly more news articles during 2017-18 before the law promulgation ($M = 3.4$, $p < .00$) and during 2019-20 after the law enforcement ($M = 1.5$, $p < .00$) than in the period of 2021-22 right after the law took effect ($M = .9$, $p < .00$). The ANOVA tests also reveal that there was a significant difference in terms of strategies used in different phases of time. The followed-up post hoc tests show that the numbers of instances of authorization strategy used during 2017-18 ($M = .38$, $p < .00$) and in 2019-20 ($M = .27$, $p < .05$) are significantly higher than that in the period of 2021-22. Meanwhile, the numbers of rationalization ($M = 1.6$, $p < .00$), denial of system shortcomings ($M = .71$, $p < .00$), and stereotyping ($M = .55$, $p < .00$) instances are significantly higher before the law promulgation than that of the during and after phase. Moralization is the strategy that significantly being used more ($M = .16$, $p < .05$) before than after the law enforcement.

Taking sub-category individually, except for justifications using rationalization of economic development and moral values, all other justifications are statistically different in use before, during, and after the law enforcement.

In the first period from 2017 to 2018, as the party-state needed to propagate and obtain the public's approval of the VCSL's introduction, state-sponsored media maximized different justification strategies, in which, the tactic of rationalizing cyber threats towards 4 main types of endangered values was most prevalent. As the top priority, more than 40% of articles in this

period justified the necessity of the law with national security protection (n= 79). The following endangered elements under cyber attacks are legitimate rights and interests of individuals and organizations (38.3%), information security (26.2%), and social stability (19.1%). The use of rationalizing national security ($M = .43$, $p < .00$), interests of individuals ($M = .38$, $p < .00$), social stability ($M = .19$, $p < .00$), and legal corridor ($M = .19$, $p < .00$) is significantly higher in 2017-18 compared to those in the latter two phases.

Media also justified the law by boosting its legitimacy with legal corridor improvement (19.1%) and economic development (10.4%). According to the media, regulations under the VCSL not only fill loopholes in the existing law system and build a more comprehensive legal corridor for cyberspace but also bring in foreign investment and economic cooperation opportunities through digital transformation. More importantly, with law conformity justification (26.8%), the media reassured that the law is aligned with Vietnam's 2013 Constitution and other international agreements regarding all socio-political and economic aspects. In addition, the law was the result of many rounds of discussion at the 14th Assembly with a high rate of approval from national delegates (86%); thus, it received positive feedback and high consensus from the public. A mere percentage of articles (7.7%) legitimized the law with moral goodness.

Furthermore, during this phase, when facing public criticism and accusations of destructive consequences of the VCSL, the national media chose to deny them all. To be more specific, they denied that the law violates freedom of expression (23%), creates business barriers (19.1%) through requirements on data localization and local office operation, gives authority more opportunities to abuse their power (12%) through individual surveillance or control of personal data (7.6%). Together with the law conformity strategy mentioned above, the media also strongly denied accusations from foreign organizations that the law violates international treaties (9.3%) that Vietnam has signed, such as the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights. A one-way ANOVA with post-hoc Bonferroni tests show that during 2017-18, the government used significantly higher number of denials regarding power abuse ($M = 1.5$, $p < .05$), business barriers ($M = 3.3$, $p < .05$), and

violation of international agreements ($M = .7$, $p < .00$) than those in the period of 2019-20 and 2021-22.

State-sponsored media not only bolster the benefits of the VCSL and defend the system in front of criticism and accusations but also deploy a backfiring strategy by portraying these dissidents with certain stereotypes. Two main targets of national media are hostile and reactionary forces (30.6%) and foreign media and organizations (24.6%). According to the media, while these reactionary forces are the main cause of cyber attacks that harm national security, infringe rights and interests of individuals and disturb social order, other foreign media and organizations have been always finding opportunities to downgrade the legitimacy of the regime. The ANOVA tests show that the use of stereotyping of hostile forces ($M = .31$, $p < .05$) and black media ($M = .25$, $p < .05$) was used significantly more frequently in the period of 2017-18.

In the second period after the law took effect in January 2019 to the end of 2020, the national media simply educated the public about the law regulations instead of giving any more justification. That was why samples collected in the period significantly dropped. However, in the third period, when the Assembly continued to draft and issue supplementary decrees to law enforcement, national media once again enhanced propaganda with similar justification strategies in the first period. It is noteworthy that during this phase, as the law has already taken effect, the state media used less of these justifications compared to that of the first period.

There are some noticeable differences between the three periods of time. First, there was a change in the priority of the party-state's rationalization of endangered values. If national security is the top priority used to justify the law during the drafting phase, the rights and interests of individuals and organizations are the first urgency in the second phase, and information security is the main reason to enforce the VCSL in the third phase. Second, law conformity was maintained as the most used justification in legitimization strategy throughout three phases of time. Third, in the second and third periods, the state media tended to use less

strategy of denying system problems. Only denial of freedom of expression violation remains highly relevant. Similarly, the media considerably less criticized hostile and reactionary forces and foreign media in the latter two periods.

Strategy	2017-18 (n= 183)	2019-20 (n= 77)	2021-22 (n= 161)
Authorization			
Impersonal authority	14 (7.7%)	5 (6.5%)	3 (1.9%)
Personal authority	8 (4.4%)	2 (2.6%)	0 (0.0%)
Authority of conformity	49 (26.8%)	14 (18.2%)	13 (8.1%)
Rationalization			
National security	79 (43.2%)	15 (19.5%)	18 (11.2%)
Information security	48 (26.2%)	12 (15.6%)	30 (18.6%)
Rights and interests of individuals and organizations	70 (38.3%)	21 (27.3%)	10 (6.2%)
Social stability	35 (19.1%)	5 (6.5%)	8 (5.0%)
Legal corridor improvement	35 (19.1%)	3 (3.9%)	7 (4.3%)
Economic development	19 (10.4%)	4 (5.2%)	12 (7.5%)
Moralization/Moral legitimation			
Moral values	14 (7.7%)	9 (11.7%)	9 (5.6%)
Cultural values/customs	15 (8.2%)	1 (1.3%)	1 (0.6%)
Denial of system problems			
Power abuse	22 (12.0%)	0 (0.0%)	0 (0.0%)
Control of personal data	14 (7.6%)	4 (5.2%)	2 (1.2%)
Violation of freedom of expression	42 (23.0%)	13 (16.9%)	20 (12.4%)
Creation of business barriers	35 (19.1%)	1 (1.3%)	2 (1.2%)
Violation of international agreements	17 (9.3%)	0 (0.0%)	2 (1.2%)
Stereotyping/Delegitimization			
Hostile and reactionary forces	56 (30.6%)	4 (5.2%)	15 (9.3%)
Foreign media/organizations	45 (24.6%)	3 (3.9%)	3 (1.9%)

Table 10. Distribution of Justification Strategies Through Three Periods of Time

Critical Discourse Analysis

Authorization

Within the domain of news media, legitimation first occurs through the adoption of legal authorization or impersonal legitimation, which defined by Van Leeuwen (2008, p.105-109), involves the acquisition of legitimacy through adherence to laws, rules, and regulations (Wang, 2022).

National media strategically invoke the constitutional framework and pertinent legal status, aligning cybersecurity regulations with these well-established laws to confer legitimacy upon the VCSL. The media characterizes it as "consistent with the Vietnam Constitution." Drawing parallels with existing legislation such as the 2005 Commercial Law, the Law of Foreign Trade Management 2017, and Decree 28/2018/ND-CP, which mandates foreign trade commercial organizations to operate representative offices in Vietnam, the media contends that the VCSL is harmoniously aligned with pre-existing legal frameworks. The party-state posits that previous laws "have been taken for granted," exemplified by the assertion that sanctions in the Criminal Law of 2017 are deemed inadequate to discipline behaviors that tarnish the nation's image and the reputation of organizations and individuals.

Secondly, besides the self-claimed authority strategy to gain internal legitimacy, the state also demonstrates international recognition and external legitimacy by allowing a global positive assessment of local governance and government activities. However, these sources of legitimacy are not formally recognised from other state or international organizations but rather vested in Western references, political elites, experts, foreign journalists and media. The state media use third-person narratives to cite these references.

> According to the newspaper, this law will create more jobs for Vietnam, as well as bring strong commitments from investors, so it is very beneficial for economic development in the country.

The state media also make use of the U.S. history of the 9/11 incident and Snowden revelation of the U.S. global surveillance to bolster the country's socio-political stability as an outcome of single-party leadership and justify the necessity of state control on cyberspace.

> The article mentioned the case in the U.S., after the terrorist attacks of September 11, 2001 and the spreading of anthrax, the country introduced a much stronger system of government surveillance following the Patriot Act. Internet and big data-related companies have grown, while the American people live under the active and close supervision of the U.S. Government. Thereby, the newspaper affirms that Vietnam is an independent country and the legislature has the right to better understand data about its citizens to protect national interests.

At the national level, when facing public opposition towards the arbitrary cybersecurity law, the government declared that the law is "not one of a kind," and that it is learned from developed and democratic nations such as the U.S. and other European countries. Gaining the law legitimacy by making references to Western experiences is also a strategy that China employed before the 2000s when setting the very first milestones for stringent internet governance (Miao & Han, 2021).

At the personal level, this kind of authority is personal or position-based authorization, which is a key aspect in the legitimation process, underscoring that the credibility derived from personal authority is contingent upon an individual's role or position within an institution (Van Leeuwen, 2007). This perspective posits that individuals endowed with higher societal status possess the capacity to wield authority, thereby legitimizing or delegitimizing actions to a greater extent than those with lower status (Rivers & Ross, 2020, p.834). The persuasiveness of such appeals is highlighted, given that individuals tend to be more swayed by sources perceived as credible, trustworthy, powerful, attractive, expert, and similar to themselves (McGuire, 1999).

National media strategically enhance the credibility of the state's claims, particularly in the context of human rights violations, by quoting foreign journalists, professors, and media

outlets. This approach is designed to add an international dimension to the media narrative, reinforcing the perceived legitimacy of the VCSL.

For instance, one media outlet cites Professor Kolotov, who asserts that the law does not infringe upon freedom of speech, thereby implying that the legal framework is endorsed even by external experts. Another media source references Dhakatribune Daily, disagreeing with opinions that the VLCS of Vietnam restricts major online platforms like Facebook and Google, potentially harming investigators's trust and disrupting the digital economy. The media frames the Vietnamese government's actions as a duty to protect citizens from potential manipulation.

By incorporating the perspectives of foreign experts and media outlets, the national media seeks to broaden the perceived support for the VCSL beyond domestic borders. This strategy aims to portray the law as not only aligned with national interests but also garnering approval from international voices, thereby bolstering its credibility on a global scale.

Thirdly, authority is gained through adherence to established norms. The legitimacy of the law extends beyond its legal foundation, encompassing robust public support characterized by a "high consensus" maintained from the initial drafting phase to its official promulgation. The law's endorsement is underscored by the orchestration of "multiple rounds of discussion and open, transparent consultations" involving lawmakers, experts, businesses, and the general public. The party and state assert a commitment to expeditiously incorporating the opinions of diverse segments of society, reflecting a spirit of respecting and listening to the people, a stark contrast to the perceived intransigence of *hostile forces* that propagate the notion that once the Party has made a decision, further discourse becomes inconsequential.

Post-enforcement, the law sustains positive feedback from both traditional media outlets and enthusiastic support from social media users. This sustained positive reception is posited as evidence that the law's content has achieved widespread acceptance and high consensus among the citizenry. In the media narrative, those expressing opposition to the law are labeled as a "minority with impure motives." The role of conformity, manifested through social validation,

group support, or peer pressures, is identified as an external force contributing to resistance to change, aligning with the insights of Lewin (1947a,b).

National media strategically employs a confirmatory strategy and external role-model legitimacy to counter assertions that the VCSL is unique, arbitrary, or totalitarian. In response to claims of arbitrariness and totalitarianism, the media emphasizes that the VCSL is not an isolated phenomenon but rather part of a broader international trend. This strategy involves affirming that the law is "not one-of-a-kind" and characterizing it as a "common trend." To reinforce this point, the media highlights the global prevalence of cybersecurity laws, citing statistics that indicate 138 countries have enacted such legislation, with 95 of them categorized as developing nations.

Moreover, the media draws a parallel with Germany's cybersecurity law, presenting it as an exemplary. By referencing Germany, the media aims to discredit opposition by insinuating that even countries perceived as democratic have implemented similar laws with potential human rights implications. The narrative suggests that the criticism from *hostile forces* opposing the National Assembly of Vietnam passing the Cybersecurity Law is easily understandable in light of these global patterns. This strategy seeks to normalize the VCSL within the context of international practices while casting doubt on the legitimacy of objections raised by dissenting voices.

The legitimization strategy employed, known as the authority of conformity, operates by emphasizing the logical premise that "everybody else is doing it, and so should you" or "most people are doing it, and so should you" (Leeuwen, 2008). This approach leverages the concept of *injunctification*, as outlined by Kay et al. (2009), wherein individuals treat descriptive norms (the way things are) as injunctive norms (the way things ought to be). This mechanism is instrumental in explaining the tendency to maintain the status quo.

The dichotomy between *is* and *ought* holds distinct ontological implications. The former aligns with materialistically oriented sciences and materialist philosophy, while the latter pertains to norms or values created by norms (Wroblewski, 1981). Subscribing to the status quo,

prevailing social-political arrangements and the legitimacy of the social system fulfills fundamental epistemic, existential, and relational needs (Jost & Van der Toorn, 2012). This acknowledgement of living within a system perceived as fair, just, legitimate, and desirable serves to reduce ambiguity, mitigate insecurity, and enhance psychological well-being, particularly among individuals with limited power and low cognitive needs. In essence, this strategy functions as a psychological mechanism to foster adherence to established norms and systems.

Rationalization

Rationalization discourse from state media represents a process of selecting particular security referent objects and answering the question of why something has to be done (Van Leeuwen & Wodak, 1999) to secure these objects. However, rationalization in this case is not to explain the VCSL promulgation itself but rather public acceptance of the law at the expense of freedom of expression and other interests.

Instrumental rationality takes center stage as the primary justification for the VCSL and its ultimate goals in regulating cyber threats targeting endangered values or security referent objects ranging from the top most important such as national security, and national defense to moderately important like public interests and social order to less important priority such as lawful rights and interests of individuals and organizations (QMN-Nguyen, 2023). The discourse employs purpose-linking words involving the infinitive *to,* such as *to ensure, to protect, to strengthen, to combat,* and future-oriented verb phrases (Fairclough, 2003, p.55) *will help, will contribute, will benefit,* and *will develop*. This rationality strategically links the law's objectives with safeguarding values ranging from national security and defence to public interests, social order, and the lawful rights of individuals and organizations.

The media discourse hypersecuritizes cyber threats, vividly depicting “multi-dimensional cyber disaster scenarios” in nearly every news article. This emphasis serves to provoke fear, instill a sense of urgency (Hansen & Nissenbaum, 2009, p. 1164), and justify the perceived

necessity of stringent cybersecurity measures. Threats on the system are among the most important contextual drivers of system justification. It triggers a need for existential satisfaction and terror prevention, with which, people restore their worth in response to threats (Branscombe, Ellemers, Spears, & Doosje, 1999; Ellemers), creating a positive illusion (Taylor & Brown, 1988) to reduce negative feeling, boost a sense of belongingness.

These threats ranged from man-made offences to hi-tech crimes. Human actors behind these threats are hostile and reactionary forces and cyberespionage aiming at carrying out plots of *peaceful evolution*, misappropriating information, revealing state secrets, spreading misinformation, disrupting national unity, insulting and slandering organizations and individuals… Meanwhile, technique-related criminals would cause ransomware and spyware attacks; phishing attacks to steal money; appropriating information of organizations and individuals for online frauds; selling personal and business data; extortion; money laundering; gambling; distribution of pornographic publications; arms trafficking; trading drugs and prohibited goods...

All these threats constitute a doom scenario of cybersecurity in the country, that it "is in the group of countries facing large-scale, high-intensity, serious and increasingly dangerous cyber attacks," and "ranked 20th among the countries in the world where the network system is attacked by malware, 8th among the top 10 countries in the world in terms of local malware infection." The portrayed threat-salient situations, on the one hand, enhance the feeling of powerlessness and dependence on the system, and on the other hand, trigger a need for existential terror prevention and fear alleviation.

Together with exaggeration of cyber threats, state media emphasize shortcomings current legal system in dealing with cyber criminals, that "the situation is extremely pressing and painful but the handling is very passive, embarrassing, and ineffective because the legal system of our country does not have a legal corridor to fully manage specific and clear regulations on illegal acts in cyberspace." In addition, the media also explicitly indicate the powerlessness of citizens

in front of these threats, for example, “personal information has been stolen without the user's knowledge.” Hence, people in cyberspace “need guidance and protection from the government.” Powerlessness boosts a sense of dependency, which is also a contextual factor that drives system justification. Outcome dependence is an independent contributor to perceived legitimacy (van der Toorn, Tyler, & Jost, 2011), thus, contributing to system-justifying bias. Prior studies showed that increased dependence on a system led participants to believe that the government is more responsible and benevolent (Kay et al., 2008), and policies related to the status quo as more reasonable and desirable compared to those not related to the status quo (Kay et al., 2009).

Against the current gloomy picture of cybersecurity in the country, the VCSL appears as a “timely, essential, proper” legal corridor to not just cope with national security threats but also to advance the business environment amidst the challenges of the Revolution 4.0. Economically, the VCSL also constitutes legal frames to smooth and benefit business operations on cyberspace as it creates “a fair competitive environment for both domestic and international enterprises” and “breakthroughs, development momentum for the economy and to utilize local’s strengths.” Furthermore, the law “brings in many more job opportunities for Vietnamese and strong partnership from investors.” This legal corridor “strictly manages the activities of cross-border service providers when doing business in Vietnam; ensures payment sovereignty, prevents tax loss for these enterprises; at the same time, eliminates inequality in business activities between foreign enterprises and domestic enterprises.”

In essence, the media's rationalization discourse strategically weaves together narratives of threat, legal inadequacy, and economic necessity to frame the VCSL as a crucial and justified response to the complex challenges posed by cybersecurity in the contemporary landscape.

Moralization

Moralization is based on values that travel among moral, aesthetic, and hedonistic domains rather than imposed by some kind of authority without further justification (Leeuwen, 2008). It is a process that promotes certain rules, norms, and behaviors (DeScioli & Kurzban

2013), with the implication for how one should behave (Salomon, Preston, & Tannenbaum, 2017). The party-state emphasizes "The fact that we are living in a civilized society, behaviors are regulated by law and human morality. Therefore, the VCSL is just a concretization of regulations in daily life, applied to the cyberspace environment." The starting point of moralization involves creating binary distinctions (Žažar, 2022) between concepts of rightness and wrongness (Rozin, Markwith, & Stoess, 1997), such as good versus bad, respect versus disrespect, or positive versus negative (Žažar, 2022). People make moral judgments based on unconscious, gut-level intuitions and emotions, with conscious reasoning primarily providing post-hoc justifications for conclusions already reached by intuition (e.g., Gutierrez & Giner-Sorolla, 2007). Moral language, especially when used by elites, is a powerful tool (Clifford & Jerrit, 2013) for shifting public debate, persuading, and motivating voters (Lakoff, 2004), as well as fostering trust, altruism, and cooperation (Haidt, 2001, 2007) within a community.

The use of modals *must, should* implies moral obligation and commitment. For example, state media emphasized, "Everyone must be responsible for their actions and statements in cyberspace."

> To fully enjoy the rights specified in the VCSL, individuals also need to ensure the fulfillment of statutory obligations. It is an obligation to comply with the law; strictly implement rights restrictions, to ensure national security, public order, and legitimate rights and interests of individuals and organizations. This is not only a political and legal responsibility, but also belongs to the ethics, and lifestyle of each person and is also the regulation of many countries around the world.

Meanwhile, the use of *will* and future-oriented language generate the audiences' optimistic scenario regarding future policy decisions (Wang, 2022). Moral legitimization gained through moralization is presented through abstraction referring to actions and practices or benefits of law enforcement. Enforcement of the VCSL is legitimized as it will "enhance awareness of community," "meet the urgent need of cyber security," and "cope with fake news and violation of fine traditions." The law aims to "raise awareness for the community about how

they should behave on the Internet to have empathy and respect for each other, to be a digital citizen with responsibility." Therefore, it is to "build an increasingly healthy, friendly, civilized and modern social networking environment in Vietnam, aiming to preserve the unique cultural values of Vietnamese people, making social networks a useful tool."

Moral evaluation is seen through the extensive use of positive, evaluative adjectives that are intertwined with rationalization and authority legitimization discourse. State-owned media praised the law promulgation and enforcement as *stringent, timely, essential, strong, legitimate, lawful, fundamental, comprehensive,* and *important*.

Excerpt on moral legitimitization strategy:

> The promulgation of the Law on Cybersecurity is extremely necessary, meeting the inevitable requirements of state management while still being consistent with the reality of social life. It is an important legal weapon to prevent and handle violations, protect national security, and maintain social order and safety.

As a part of the legitimization and delegitimization strategy, moral value comparisons are also made to contrast the boundary between what is good and what is not. On the one hand, whenever regarding either the cybersecurity law, legal corridor, or citizen rights, state media bolster and tag along with positive adjectives such as *legitimate, lawful, fundamental*, and *comprehensive*. On the other hand, national media use negative adjectives such as *black, alien, distorted, unacceptable, and opportunistic* for any individuals or organizations that criticize and oppose the law. They are labeled as "opportunists, hostile and reactionary forces" with a "distorted mentality." Media accused foreign internet operators as "uncooperative and unfriendly" if they are hesitant to provide or delay the provision of relevant data upon the Government's requests. Foreign media that said the law "forced people to comply with rules that violate people's legitimate freedom of expression on social networks at will" are called "black media" with "distorted discourse", thus, are "unacceptable." Targeting dissidents, the state media

accused that they only "worsen the unsafe reality of the country in cyberspace; and this does not only cause risks for the sovereignty in cyberspace but also the real sovereignty in real life."

Denial of System Problems

Denial, as a communicative strategy, is not limited to individual and interpersonal behavior but extends to institutional levels. Within the discourse of denial, various tactics are employed for purposes such as positive self-presentation, face-saving, defence, non-monotonic correction, excuse, provocation, blaming, discounting, mitigation, or reversal (van Dijk, 1992). The overarching objective of employing denial strategies is to avert and rectify negative impressions of the speaker or impede the formation of negative inferences among the speaker's audience (van Dijk, 1992). Functioning within a socio-political context, denial discourse becomes integral in managing resistance, dissent, and opposition, serving as a strategic element in the perpetuation of hegemony (Lauren, 1988). Denial can manifest either explicitly or implicitly.

In the context of the state media's response to accusations and suspicions related to the VCSL, the predominant denial strategy employed is direct denial. This is evident in the state media's use of negative claims, such as "So there is certainly no abuse of power here," and affirmative adverbs like *definitely, certainly, absolutely,* and *clearly*. Key debates surrounding the VCSL include concerns about potential power abuse among law enforcement bodies, government control and scrutiny of personal data, violations of freedom of expression and international agreements on human rights protection, and the creation of business barriers, especially for foreign companies.

The state media utilizes direct denial statements to establish the truth by refuting accusations and dispelling doubts (van Dijk, 1992). The denial discourse in this strategy employs both absolute negative terms, like "not true," and euphemisms such as "inaccurate," "distorted," and "misunderstood." For instance, the media counters claim about the VCSL creating business barriers by stating, "there has been a lot of inaccurate information on the Internet, social

networks said that the VCSL will create business barriers, increase costs and sub-licenses for businesses."

Direct denial statements are often followed by more detailed corrections, emphasizing legal regulations or delineating boundaries in law enforcement. The attribute word *only* is frequently employed to specify the scope of the law's enforcement. For example, statements such as "a specialized network security agency only supervises illegal acts in cyberspace" and "the law only focuses on information systems that are important to national security" serve to set limitations on the law's reach.

The combination of negative terms and correction aims to strengthen the denial discourse. For example, addressing the accusation of international agreement violation, the media emphasized the VLCS "does not violate international agreements" as "international agreements such as GATT 1994, GATS, TRIPS, CPTPP always have exceptional regulations about security that allows nations to pursue the national security at the highest level," and "no international commitments are forcing us to sacrifice these (national) interests." Even with the less arbitrary regulations like Code of Conduct on social media and Code of Conduct of journalists on social media "does not go against the commitments of the State in ensuring personal freedom and freedom of business under international treaties to which Vietnam has acceded," and have no discrimination "between service providers, users and consumers resided in the country or abroad."

As part of the denial strategy, the state media adopts a more forceful form, reversal or transferring the charge to others (van Dijk, 1992). When addressing laypeople, the media not only denies the drawbacks or consequences of the law but also attributes misunderstandings to them, stating they "do not understand" or "do not read the law carefully." When addressing businesses and agencies expressing concerns about data surveillance and sublicense requirements, the media criticizes them, suggesting they fear inspection due to a lack of understanding or involvement in opaque business practices. Meanwhile, critics are labeled as

enemies, reactionaries, and hostile forces who “take advantage of public ignorance to incite and confuse public opinion,” even when the state media admitted existing shortcomings of the VCSL and the system.

> In fact, no state is absolutely perfect, because the State is an organization formed and developed by people. This model will still have shortcomings such as corrupt bureaucracy, moral degradation of a few leading cadres… However, that does not mean that a few "worms" are equated with common shortcomings…Political opportunistic forces have focused on exploiting information about shortcomings, limitations, and failures of the Party and State in the fields of economy, culture, society, security and defence.... At the same time, the forces tried to take advantage of the shortcomings of a part of the cadres and party members who were degraded, corrupt, and negative and were disciplined to raise the individual phenomenon to its essence, blacken the regime, and deny efforts and achievements of the whole political system.

Denial of human rights violations is the party-state’s most defensive reaction. The leaders not only take into account the terms violations and injustice reduction themselves but also link any criticism to international competition and attacks from hostile and reactionary forces. By framing these attacks as “spreading false information, distorting, defaming, denying the government; fabricating, causing confusion among the people; distort history; denying revolutionary achievements” and even more serious as “sabotage internal affairs, incite protests, and overthrow the regime,” it allows the party-state transfer the charges to hostile forces and invite co-opt vocal cyber-nationalists with defensive nationalist rhetoric as well as triggering motives to defend the nation among public (Jones, 2022). The author argues that the reversal strategy benefits the party-state as it makes the population see the individual human rights issues as national issues and international competition against national interests; thus, making them focus on the threat to the nation’s standing rather than the human rights issue itself (Jones, 2022). Empirical studies utilizing theories of motivated reasoning and social identity reaffirm the argument that the Chinese public perceives foreign criticism of China's human rights records as a defence against hostile outsiders. The motive is even strengthened, as state discourse is salient as

the state mainstream is the only option in the country while competing discourse is controlled and eliminated through content censorship and blockage of external sources.

> In the so-called reports on the human rights situation in Vietnam over the years, a phrase often appears, which is "Vietnam continues to violate freedom of speech and freedom of the press". This tone, if compared with the reality of the development of the press in Vietnam today, no one understands what it is based on.

Furthermore, the state media marginalizes and classifies these groups as a “minority with impure motives,” contrasting them with the “high consensus among citizens,” aiming not only to “defend us against them” but also to “debilitate resistance” (T. van Dijk, 1992) against the law.

Stereotyping/Delegitimation

Stereotypes serve an ideological function, especially for in-group members to justify the dominance or exploitation of advantaged groups over disadvantaged groups (Jost & Banaji, 1994). This is used to explain why people accept existing economic or socio-political arrangements as well as the positions and actions of self and others (Jost & Banaji, 1994) even when the system disadvantages them. As the authors explain, this tendency arises from people's inclination to form ideas about characteristics, attribute traits to themselves and others, and choose social roles that align with existing arrangements or outcomes, whether positive or negative, rather than question the order or legitimacy of the system. This tendency applies to both the powerful and powerless when stereotyped. This standpoint of the SJT has been contested in a variety of contexts with different kinds of systems including socio-economic ladder (e.g., see Baryla et al., 2015; Day & Fiske, 2017; Gampa, 2018), religious system (e.g., see Friesen et al., 2019), gender discrimination (e.g., see Froschauer, 2016), relationships (e.g., see Day et al., 2011), and organizational structures (e.g., see Murray, 2015).

Blaming oneself and the in-group for negative consequences is a crucial mechanism for maintaining the belief that people get what they deserve (Jost & Banaji, 1994).

Delegitimation, which is an extreme case of stereotyping and prejudice (Bar-Tal, 1990), is the third most important strategy with 126 instances targeting two main subjects: reactionary, hostile forces and black media. These forces are defined as those who are against the regime, distort information, and obstruct the implementation of the law. Delegitimation strategy presents how the state responded to social resistance and justified suppression towards dissidents. Compared to other types of autocratic regimes, single-party regimes are most active in legitimizing their rule and propping themselves up as well as delegitimizing their rivals (Dukalskis & Patane, 2019).

Political labels and trait characterization are most used tactics for delegitimation. The main label "hostile and reactionary forces" has been used consistently in media discourse across state-sponsored outlets indicating individuals and groups who are characterized as "democratic," "oppositional," and "opportunistic" resided not just "at home" but also "overseas." Upon different contexts, other equivalent labels are also used. When referring to the law resistance as a violation of law, state media criminalized these forces as "criminals" and "extremists" as they "commit acts of sabotage, infringe upon and threaten social order, property of the State, agencies, organizations and individuals, and the existence of the regime." When referring to the law resistance as a violation of social order and norms, media called hostile forces "instigators, agitators, troublemakers, bad elements" who used "cunning and sinister tricks" with "dark motives" to "mix real and fake information, spread rumors, and attract attention," "smearing, fabricating, and discrediting the image of comrades leading the Party and State," and to "seduce and give money to entice people to participate in protests and cause trouble," or taking advantage of "people's patriotism," "cause skepticism and divide the great national unity." Political leaders often called dissidents and protest participants as "extremists and social disrupters" that galvanized by foreigners (Tien Thang, 2018; Le Kien, 2018).

State media also name and shame particular human rights groups such as Việt Tân, Triều Đại Việt, other international organizations including Amnesty International, Freedom House, Human Rights Watch, or Reporters Without Borders, and other foreign media such as BBC,

RFA, VOA, RFI. State media delegitimized these groups and organizations in terms of their reputation and activities. Due to their criticism and oppositional views on the VCSL, they are portrayed as uncooperative, unfriendly, one-sided, misleading forces which hide in the shadow of press freedom and human rights to carry out *color revolution, street revolution, peaceful evolution*… aimed at weakening and abolishing the political regime in our country by disrupting the country, calling for international intervention, denying the leadership role of the Party, and promoting reactionaries and political opportunities. Freedom House is the most heavily criticized organization. According to state media, this organization "has a very weak reputation in Europe," and "freedom of the press only appears in the countries they want, the institutions they like, it has nothing to do with the reality that is happening." Freedom House and other organizations are also evilifized not just in what they did but also in their deeds as the nature of their works is "changing white for black and turning yes to no" about freedom of speech and press freedom in Vietnam.

All of these stereotypes reflect perceived threats that turned into state-sponsored media discourse. Perception of threat and delegitimization form a vicious cycle (Bar-Tal, 1990), in which, perceived threats feed delegitimization, and delegitimization, in turn, breeds and justifies exceptionally preventive acts that make delegitimization even more salient. This is also a conflict model due to the far-reaching incompatibility of goals proposed by Bartal in his works (Bar-Tal, 1990). However, delegitimation, in this case, does not involve a high degree of violence but rather perceived threats and hostility. As a consequence, delegitimization is both a reaction of the threatened group towards the threatening group (e.g., see Krauss & Deutsh, 1966) and an input of justification for the delegitimizing group to perform exceptional acts towards the delegitimized group (e.g., see Sheriff, 1966).

From the audience perspective, delegitimization in media discourse breeds and ideologically maximizes the distinction between us and them (Bar-tal, 1990) by emphasizing irreconcilable or incompatible goals, upholding the perception of threats, disrupting the sense of security, thus, maintaining group uniformity and strengthening the belief that the delegitimized

group deserves negative attitudes and behaviors (Bar-tal, 1989). By emphasizing the boundary between us and them and portraying them as *threat*, delegimization discourse fosters the sense that undemocratic or exceptional measures are just a method of self-defence (Bar-tal, 1989).

7.4. Reflection on SJT

The party-state and state media utilize a range of justification strategies to elevate system justification motives and reinforce the legitimacy of the VCSL and the broader political regime. Through authorization, rationalization, moralization, denial of system problems, and stereotyping and delegitimation, the media crafts a compelling narrative that encourages public acceptance and support of the existing system. These strategies work in concert to maintain social order, suppress dissent, and foster a sense of stability and continuity, thereby ensuring the longevity and resilience of the current political structure.

Authorization draws on the perceived legitimacy of both impersonal and personal authorities. By referencing established legal frameworks, the Constitution, the Penal Code, and international agreements, the state media creates a sense of legitimacy rooted in legal and institutional norms. Additionally, invoking the authority of elite figures and experts lends personal credibility to the law. This strategy reinforces the belief that the current system operates within a legitimate and recognized legal framework. By aligning the VCSL with authoritative sources and figures, the media encourages the public to see the existing political and legal structures as just, necessary, and credible. This alignment helps mitigate doubts and opposition, fostering a sense of stability and continuity in the current system.

Rationalization emphasizes the practical benefits and necessity of the VCSL. The media frames the law as crucial for protecting national security, information security, the rights and interests of individuals and organizations, and social stability. The law is also portrayed as a catalyst for economic growth and foreign investment. By highlighting the pragmatic and beneficial aspects of the VCSL, this strategy encourages the public to perceive the existing system as effective and efficient in addressing contemporary challenges. The focus on tangible

benefits and solutions reinforces the belief that the current political and legal arrangements are well-equipped to handle threats and opportunities, thereby reducing the impetus for change and enhancing acceptance of the status quo.

Moralization involves framing the VCSL and the actions of the state as morally right and aligned with societal values. The media uses moral language to describe the law and emphasizes the moral obligations of citizens to comply. This strategy appeals to cultural values and norms, presenting the law as a reflection of the collective moral compass. By embedding the law within a moral framework, the state encourages citizens to view compliance as a moral duty. This moral framing aligns individual behavior with broader societal values, promoting a sense of collective responsibility and ethical governance. The moralization of the law thus strengthens the perception that the existing system is not only practical but also ethically sound and deserving of support and preservation.

Denial of system problems involves refuting criticisms and accusations against the VCSL. The state media employs direct denial statements to counter claims that the law infringes on freedoms, creates business barriers, or violates international agreements. By asserting alignment with international treaties, the media aims to negate allegations of human rights violations. This strategy serves to protect the image of the state and its legal framework from negative perceptions. By denying system problems, the media mitigates threats to the legitimacy and credibility of the current system. This denial helps maintain public trust and confidence in the system, thereby reducing cognitive dissonance and fostering acceptance of the status quo as fair and just.

Stereotyping and delegitimation involve discrediting and marginalizing opposition to the VCSL. The media labels dissenting voices as hostile forces, criminals, and opportunists, portraying them as threats to national security and social order. This strategy creates a clear dichotomy between the compliant, patriotic citizens and the disruptive, dissenting elements. By demonizing opposition and framing it as morally and politically illegitimate, the state

discourages dissent and fosters conformity. This strategy reinforces in-group solidarity and out-group antagonism, making the existing system appear more cohesive and just by comparison. The clear distinction between *us* and *them* helps elevate the status quo by portraying it as the protector of societal values and stability against subversive elements.

Chapter 8. Conclusion

8.1. Main Findings and General Discussion

Built in SJT, this thesis's overall purpose is to examine institutional evidences used by the party-state to justify the contentious promulgation and enactment of the VCSL since 2018. The institutional clues include contextual and dispositional attributes that the political leaders exploit and convey through the government's mouthpiece, the state-sponsored media, to trigger, motivate, and resonate with resident's psychological and behavioral tendency to justify the system and its political arrangement even at the cost of citizens's rights. The study's findings can be comprehensively understood through the lens of the SJT.

The Study 1 shows a stark contrast between the narratives presented by state-sponsored and international media regarding the VCSL. Taking a counter-argument and criticism approach, the international media focus on the potential human rights abuses and economic drawbacks of the VCSL, reflecting broader concerns about the law's implications for freedom of expression, privacy, and international business operations. Meanwhile, the state media heavily employ securitization and hypersecuritization grammars to portray existential threats on cyberspace lesser than an issue of human security but rather a matter of death and survival of a country in terms of national security, network security, political stability, and social order. By constructing a narrative of existential threat, the media leverage a fundamental psychological mechanism: when individuals perceive their safety or societal stability to be at risk, their motivation to justify and defend the existing social order intensifies. This dynamic is rooted in the need for security and certainty, driving public support for measures that promise protection and stability. The emphasis on imminent threats creates a sense of urgency and necessity, making the VCSL appear not only rational but imperative.

Against the gloomy scenario of a world without cybersecurity, emphasizing legitimation, state-sponsored media heavily emphasize themes related to national security, legal legitimacy, and economic development. This framing suggests a deliberate effort to portray the law as

essential for national security and public order, to shape public perception and justify political arrangements in Vietnam, and subsequently, reinforce state power. This narrative strategy effectively mitigates potential resistance to the law by framing it as a critical response to pressing dangers, thereby enhancing the perceived legitimacy of not only the state's actions but also the ruling regime.

After creating a sense of existential threats, the portrayal of the VCSL as indispensable for achieving positive outcomes such as enhanced security, economic growth, and the protection of individual rights cultivates a sense of dependence on the existing system. This strategy taps into the concept of outcome dependence, which suggests that when individuals perceive their well-being and success to be closely tied to the current system, their support for that system increases. By emphasizing the beneficial impacts of the VCSL, state-sponsored media foster a narrative that links individual and collective prosperity to the maintenance of the status quo. This approach aligns with empirical findings that suggest heightened dependence on a system enhances its perceived legitimacy and support. The media's focus on the law's potential to drive economic development and safeguard personal rights reinforces the notion that the VCSL is not merely a regulatory measure but a foundational component of societal well-being. This narrative positions the state as a benevolent protector and provider, further entrenching public support.

Critically, state-sponsored media present the VCSL as a natural extension of Vietnam's long-standing commitment to security and stability. By framing the law as part of a continuous effort to uphold national integrity, social order, and legal platform, the media reinforce the perception that the existing political system is both natural and beneficial. This strategy aims to reduce cognitive dissonance by aligning new policies with established values and practices, promoting the acceptance of these policies as logical and necessary extensions of the current system. This narrative approach supports the maintenance of the status quo by normalizing the VCSL within the broader context of Vietnam's historical and cultural commitment to stability. It suggests that the law is not a radical departure but a reinforcement of familiar and trusted principles. This finding is reinforced in Study 3, where the law conformity or normalization of

the new norm has been found a prevalent tactic employed by the party-state since the drafting of the VCSL to its enactment. By embedding the VCSL within the narrative of national continuity and resilience, the media foster a sense of coherence and inevitability, which diminishes resistance and fosters compliance. This narrative tactic ensures that the public views the VCSL as a legitimate and integral part of the nation's ongoing quest for security and development.

If Study 1 provides an overall presentation of the VCSL on state-sponsored media and introduces contextual factors that trigger motivations for system justification, Study 2 delves into a more latent layer of psychological mechanism, exploring how the party-state makes the dispositional attributes congruent with a sense of powerlessness, political allegiance, and a feeling of alienation of hostile forces.

Opposite to the death-threatening cyber doom, one of the core findings in Study 2 is the portrayal of powerless and vulnerable ordinary citizens, especially internet users. The media emphasizes the technical, functional, and most importantly political ignorance of users, painting them as easily manipulated and victimized by cybercrimes and hostile forces. This narrative of powerlessness can trigger cognitive dissonance and enhances the perceived legitimacy of the VCSL among the public, motivating them to support and justify the existing socio-political arrangements as outlined by the state. This strategy leverages existential threats to national security and personal safety, reinforcing the need for a strong, protective government.

The sense of powerlessness is heightened by the portrayal of an inescapable shared reality, where cyber threats are depicted as pervasive and indiscriminate. This framing satisfies both epistemic and relational needs, providing a collective understanding of the status quo and fostering social cohesion. By emphasizing that no individual or nation is immune to cyber threats, the media justifies the stringent measures of the VCSL as necessary for collective security. This shared reality aligns public perception with the state’s narrative, reducing cognitive dissonance and promoting system-justifying beliefs. The portrayal of a dangerous and

chaotic cyberspace without the VCSL reinforces the necessity of the law and the state's role as the guardian of national and individual security.

Additionally, the study highlights how the media promotes unwavering political allegiance to the VCP by linking patriotism and national duty with support for the VCSL. The media frames dissent and criticism as morally and politically wrong, associating them with hostile and reactionary forces. This alienation of *them* serves to delegitimize opposition and justify the suppression of dissent. By portraying hostile forces as threats to national security and societal stability, the media rationalizes the need for the VCSL and other restrictive measures. This narrative creates a clear distinction between the loyal, patriotic citizens who support the state and the dangerous, subversive elements who oppose it.

Study 3 identifies key justification strategies, including rationalization, moralization, authorization, denial of system shortcomings, and stereotyping/delegitimization. Each of these strategies contributes to a broader ideological framework that supports system justification and mitigates opposition. These justification strategies are not isolated but interconnected, each reinforcing the others to create a robust ideological construct.

By rationalizing the VCSL as a necessary response to cyber threats, the media appeal to public reason and pragmatism, making it difficult for citizens to oppose the law without appearing irrational or unpatriotic. Moralization further strengthens this acceptance by framing compliance with the law as a moral duty, aligning it with societal values and norms. Authorization enhances the law's perceived legitimacy through references to authoritative sources and legal frameworks, while denial of system shortcomings addresses potential criticisms, protecting the state's image. Finally, stereotyping and delegitimizing dissenting voices marginalize opposition, creating a clear dichotomy between compliant, patriotic citizens and disruptive elements.

These strategies collectively support system justification by promoting the perception that the existing social and political arrangements are just, legitimate, and necessary. They can

mitigate cognitive dissonance among the public, ensuring that even those disadvantaged by the system perceive it as fair and beneficial. This comprehensive approach underscores the role of media discourse in influencing public perception and maintaining political stability in authoritarian contexts.

A critical element consistently present throughout the justification discourse in state media is the portrayal of hostile and reactionary forces and their alleged threats to national security and the regime. This element plays a crucial role in justifying the VCSL and reinforcing the ruling regime's legitimacy and carries several significant implications.

First, although the party-state attempts to frame the justification of the VCSL in terms of human security emphasizing the protection of citizens' rights, interests, and safety, the discourse is predominantly characterized by hypersecuritization. The use of heavily war-related language underscores a pragmatic approach centered on the survival of the VCP and the regime. This securitized narrative, which evokes imagery of war and conflict, shifts the focus from individual security to regime security, thereby justifying stringent measures under the guise of protecting the state from existential threats.

Second, despite the state's official stance denying that the VCSL is intended to strengthen the Penal Code for handling hostile acts, and to increase censorship and surveillance activities, the overemphasis on hostile and reactionary forces in the media discourse suggests otherwise. The persistent narrative of threats from these forces indicates that the primary justification for the VCSL revolves around national security, social order, and political stability. This contradiction highlights the underlying motive of consolidating state power and controlling dissent under the pretext of addressing external and internal threats.

Third, the portrayal of hostile and reactionary forces in state media discourse underscores the unchanging and persistent ideology and fear among political leaders since the Renovation (Đổi Mới) policy was introduced in 1986. This enduring fear of destabilization and opposition has shaped the state's approach to governance and legal frameworks, leading to the consistent use

of security threats as a rationale for restrictive laws like the VCSL. The continual invocation of these threats serves to legitimize the regime's actions and policies, reinforcing the narrative of an ever-present danger that necessitates authoritarian control.

8.2. Contribution to Existing Literature

This study is the first systematic investigation of cybersecurity discourse in Vietnam and is pioneering in its examination of how different justification strategies are employed by the Party-state to mitigate public criticism of the controversial VCSL. While legitimation is crucial for the survival of authoritarian regimes and the monopoly power of the VCP, existing literature has primarily focused on general strategies employed by the regime and the Party. This study, however, zooms in on the specific narrative and legitimation process of the VCSL, systematizing these strategies and theorizing them into a broader foundational framework.

It is important to emphasize that the study is not designed to investigate psychological mechanism for system justification according the traditional bottom-up approach of the theory but to provide institutional evidence on how advocates deploy narratives to amplify or dampen system-justifying motives and motivated social cognition (Jost & Hamilton, 2005). The study, therefore, does not aims to provide direct empirical findings to testify theory hypotheses but making theoretical inferences and exploration from the institutional approach on how the system justification is operated within specific contexts and what else to observe in the interplay of psychological drivers, historical, cultural factors, and state-led ideological work (Cao & Quian, 2023) for manufactured consent.

By extending the SJT's scope looking into institutional discourse, the study demonstrates that system justification is also a process where the powerful entities including government, media, and political elites actively engage to construct, create, and reinforce narratives and beliefs maintain system legitimacy and public compliance. In a more specific context, the integration of the SJT into the legitimization of the VCSL unveil a logic of authoritarian societies, in which a set of subject positions, objects, and and a system of meaning are

constructed liking subjects and objects to institutional settings (Garcia Santamaria & Salojärvi, 2020).

Manipulation of Manufactured Threats and Shared Reality

The most prominent findings in this study highlight the manipulation of manufactured threats and the construction of a shared reality prevailing in media discourse. These two components play pivotal roles in triggering epistemic, existential, and relational needs, yet they are rarely described in detail within the framework of the SJT.

By manipulating threats, power structures create an environment where people feel vulnerable, insecure, and threatened, compelling them to turn to well-established systems for stability. As a result, individuals are more likely to support and tolerate restrictive policies and social arrangements. In the context of Vietnam's VCSL enforcement, threats are less often framed within a technical axis and are more boldly embedded in cultural or moral narratives, with specific scapegoats—such as dissenters or foreign influences—portrayed as threats to societal values or national identity.

These threats are used to trigger system justification mechanisms and are tied to feelings of personal vulnerability stemming from deteriorating safety, economic conditions (Garcia Santamaria & Salojärvi, 2020), cultural fabric, and moral integrity. Constructed threats are presented not merely as survival issues but as pervasive problems beyond individual control, fostering a sense of powerlessness and dependence. This ensures that authorities appear as the only viable source of protection and social coherence. Manufactured threats, therefore, cultivate a public dependency on the system for safety, aligning with SJT's premise that individuals are motivated to justify the system when they see it as indispensable.

This analysis reveals that instead of relying on organically occurring threats, states actively create or amplify certain dangers to sustain this dependency. This demonstrates that

system justification can be a top-down, strategically induced process, rather than a purely psychological or internally motivated phenomenon.

Through media discourse, states construct a shared reality by presenting a unified narrative around these manufactured threats. By controlling information, governments ensure citizens develop a collective understanding of what is deemed "real" and "true" about these threats, aligning public perceptions with state interests. While SJT traditionally assumes that individuals justify systems based on personal experiences and beliefs, the creation of a shared reality suggests that governments can engineer a collective mindset, making system support seem widely accepted and, therefore, legitimate.

Cognitive Dissonance Management

Cognitive dissonance is a driving mechanism for system justification typically studied through surveys, experiments, and measures of cognitive, psychological, or behavioral responses at both conscious (e.g., Jost et al., 2003) and unconscious levels (e.g., Jost, Sapolsky, & Nam, 2018). However, it is not a self-derived mechanism; contextual conditions play a significant role. This study demonstrates how media actively engage in shaping and influencing this mechanism by incorporating cognitive dissonance management into their discourse. This management involves generating information that facilitates conflicting beliefs and messages to reduce or prevent discomfort.

The findings suggest various media framing strategies that drive this mechanism. For instance, framing hostile forces as the primary cause of cyber threats and portraying opposition as unpatriotic reduces dissonance among those who might otherwise question cybersecurity regulations. This makes compliance appear as the socially responsible choice. Similarly, by positioning the leadership of the party-state as a benevolent protector, narratives align individuals' sense of security with state authority, making them less likely to question the legitimacy of restrictive policies. Furthermore, by justifying cybersecurity restrictions as

reasonable and legitimate, narratives help people reconcile their support for these policies with their rights to privacy and freedom of speech.

This study enriches SJT by illustrating that system justification is not merely a psychological tendency but can be systematically cultivated through institutional discourse. Media not only feed but actively shape these psychological needs, broadening SJT's perspective from an individual-driven process to one deeply intertwined with institutional control. The state's use of media to suppress dissonant beliefs and reinforce favorable interpretations turns system justification into a managed process, guiding citizens toward system-supportive beliefs rather than allowing them to form these independently.

Suppression of Counter-Narratives

This study reveals that the suppression of counter-narratives is not merely an act of censorship but is framed within a moral framework that portrays dissent as fundamentally dangerous or corrupting to societal values. By framing opposition as morally suspect or a threat to the cultural or ethical foundations of society, the state encourages citizens to view support for the system not just as a rational choice but as a moral imperative. This framing positions system support as the "patriotic" or "loyal" path, while dissenters are depicted as misguided, morally deficient, or even traitorous.

Through this strategy, the state leverages citizens' ethical identities, fostering a climate where rejecting dissent is seen as upholding societal good. Individuals are not only dissuaded from engaging with alternative perspectives but actively distance themselves from these views, perceiving counter-narratives as morally offensive or dangerous rather than simply oppositional.

This analysis contributes a critical moral dimension to SJT, suggesting that system support can be rooted in moral conviction rather than just fear of instability or pragmatic acceptance of the status quo. While SJT traditionally emphasizes psychological motives such as the need for stability or security, this study demonstrates that system justification is deeply tied to moral and ethical alignment. By framing system support as an act of personal and collective

virtue, states amplify loyalty through emotional and ideological commitment. In contexts where dissent is portrayed as morally harmful, this study expands SJT's scope to include the power of state-driven moral narratives, which foster a strong, value-based allegiance to the system. This moralization enhances system resilience, making individuals more resistant to counter-narratives and reinforcing the system's legitimacy at an ethical level.

Role of Framing and Priming

The study underscores the critical role of framing and priming in reinforcing system justification, particularly within state-controlled media discourse. By analyzing how the Vietnamese government uses media to shape public attitudes toward the VCSL, the study demonstrates how these mechanisms actively cultivate system-supporting beliefs and align public perceptions with state objectives.

Framing emerges as a key tool for shaping public perceptions by portraying cybersecurity as an existential threat and positioning the VCSL as a necessary safeguard against foreign interference and internal instability. This aligns with the SJT by fulfilling existential needs for security and epistemic needs for certainty, making the law appear as a logical and essential solution to perceived dangers. The narratives emphasize themes such as moral obligation, societal protection, and national sovereignty, reinforcing the perception of the system as benevolent and indispensable. Priming plays an equally significant role, as repetitive messaging ensures that system-justifying beliefs remain salient and readily accessible to the public. State media consistently amplifies the necessity of the VCSL, creating a cognitive environment where individuals are more likely to align with the system. This repetition solidifies public compliance, showing how priming enhances the ease with which citizens adopt system-supportive views.

Moreover, the study reveals how dissent is framed as a threat, with opposition to the VCSL depicted as morally and socially harmful. This framing suppresses alternative viewpoints, reduces cognitive dissonance, and minimizes resistance to the system. By casting dissenters as destabilizing or foreign-influenced, the government delegitimizes counter-narratives, positioning

itself as the sole protector of stability and national values. Moral framing further strengthens public alignment with the state by presenting compliance with the VCSL as a duty to protect societal values. This approach satisfies relational needs by fostering a sense of ethical obligation and social conformity, making citizens more likely to perceive compliance as a moral and socially accepted norm. Through this moral framing, the state deepens public loyalty and diminishes support for resistance.

The study extends SJT beyond individual psychological processes by demonstrating how framing and priming are not only internal mechanisms but are actively engineered by institutions to manufacture consent. By focusing on top-down, state-led narratives, the study shows how powerful actors like the Vietnamese government strategically trigger psychological motivations for system support.

Furthermore, this study extends the scope of SJT beyond social, cultural norms and beliefs, and economic and political structures to include the justification for enforcing a new law. Examining the justification for the VCSL provides insights into broader political practices of the regime, moving from specific policy-level justifications to overarching regime legitimacy. While SJT mainly focuses on psychological attributes, this study provides a detailed analysis of power and ideology through language and framing. It highlights the critical role of language in forming justifications, demonstrating how state-sponsored media uses language to construct and perpetuate ideological narratives.

In addition, although justification is a central tenet of SJT, there has been a lack of systematization regarding how a system organizes and develops certain ideologies into different justifications. This study addresses this gap by categorizing and analyzing specific justification strategies used by the state to legitimize the VCSL. Traditionally, SJT has been explored through quantitative methods such as surveys and experiments on human subjects. This study employs both qualitative and quantitative methods to examine discourse, offering a richer and more

nuanced understanding of how justification strategies are constructed and disseminated through state-sponsored media.

8.3. Limitations and Future Research

While this study provides significant contributions to understanding the justification strategies for the VCSL in Vietnam and theoretically contributes to SJT, some limitations are unavoidable. These limitations include the potential lack of generalizability, methodological constraints, temporal limitations, and limited exploration of audience reception. Addressing these limitations in future research could provide a more comprehensive and nuanced understanding of the complex interplay between media discourse, public perception, and political legitimacy.

One of the primary limitations of this study is its focus on the Vietnamese context, which may limit the generalizability of the findings to other authoritarian regimes or different political systems. The unique political, cultural, and historical factors in Vietnam might influence the nature and effectiveness of the justification strategies employed. Thus, while the study provides valuable insights into the VCSL and the legitimization strategies of the VCP, these findings may not be directly applicable to other contexts without considering local specificities.

In addition, while comprehensive in covering the period before and after the implementation of the VCSL, the temporary scope of this study may miss longer-term shifts in discourse and public perception. Changes in political dynamics, socio-economic events, and technological advancements could influence the discourse over time, requiring ongoing analysis to capture these evolving narratives.

Finally, while the study extensively analyzes the content and strategies of state-sponsored media, it does not provide insight into how these messages are received and interpreted by the general public. A lack of confirmation for the motivated system justification mechanism from the target audience might make the thesis's findings less objective. Understanding the audience's reception, resistance, or acceptance of these narratives would provide a more nuanced view of

the effectiveness of the justification strategies. Future research could incorporate audience-focused research to triangulate with a discourse analysis from an institutional perspective.

BIBLIOGRAPHY

Abulof, U., & Kornprobst, M. (Eds.) (2017). *Communication, legitimation and morality in modern politics: studying public justification*. Routledge.

Abuza., Z. (2015). Stifling the public sphere: Media and civil society in Vietnam. National Endowment for Democracy and International Forum for Democratic Studies.

Adorno, T. W., Frenkel-Brunswik, E., Levinson, D. J., & Sanford, R. N. (1950). *The authoritarian personality*. Oxford, England: Harpers.

AFP. (2019, December 9). Vietnam's draconian cybersecurity bill comes into effect. The Straits Times. Retrieved from https://www.straitstimes.com/asia/se-asia/vietnams-draconian-cybersecurity-bill-comes-into-effect

Agius, C. (2019). Social Constructivism. In *Contemporary Security Studies* (5th ed.). Oxford University Press.

Aljazeera. (2020, April 22). Facebook versus Vietnam: Censorship wins. Retrieved December 10, 2022, from https://www.aljazeera.com/economy/2020/4/22/facebook-versus-vietnam-censorship-wins

Al-Tahmazi, T. H. (2015). The pursuit of power in Iraqi political discourse: unpacking the construction of sociopolitical communities on Facebook. *Journal of Multicultural Discourses*, *10*(2), 163–179. https://doi.org/10.1080/17447143.2015.1042383

Amnesty International. (2020, April 22). Viet Nam: Facebook must cease complicity with government censorship. Retrieved December 10, 2022, from https://www.amnesty.org/en/latest/news/2020/04/viet-nam-facebook-cease-complicity-government-censorship/

Anh, T. (1994). Process of economic policy reform. In V. T. Anh (Ed.), *Vietnam's Economic Reform: Results and Problems* (p. 22). Ha Noi: Social Science Publishing House.

Aradau, C., & van Munster, R. (2007). Governing terrorism through risk: Taking precautions, (un) knowing the future. *European Journal of International Relations, 13*(1), 89–115.

Aronson, E. (1969). The theory of cognitive dissonance: Current perspective. In L. Berkowitz (Ed.), *Advances in experimental social psychology*, Vol. 4 (pp. 1–34). New York, NY: Academic Press. https://doi.org/10.1016/s0065-2601(08)60075-1

Asia Sentinel. (2019, December 14). Draconian Viet Cybersecurity Law Due Jan. 1. Retrieved December 10, 2022, from https://www.asiasentinel.com/p/draconian-vietnam-cybersecurity-law

Altemeyer, B. (1996). The authoritarian specter. Cambridge, MA: Harvard University Press.

Azevedo, F., & Jost, J. T. (2021). The ideological basis of antiscientific attitudes: Effects of authoritarianism, conservatism, religiosity, social dominance, and system justification. *Group Processes and Intergroup Relations*, *24*(4), 518–549. https://doi.org/10.1177/1368430221990104

Babb, C. E. (2022). Digital dictators: How different types of authoritarian regimes use cyber attacks to legitimize their rule. (Unpublished thesis, Norman Paterson School of International Affairs, Carleton University).

Backman, S. (2022). Risk vs. threat-based cybersecurity: the case of the EU. *European Security, 0*(0), 1–19. https://doi.org/10.1080/09662839.2022.2069464

Badarneh, M. A. (2020). Discourses of defense: Self and other positioning in public responses to accusations of corruption in Jordan. *Discourse Studies, 22*(4), 399–417. https://doi.org/10.1177/1461445620914670

Bahamondes, J., Sengupta, N. K., Sibley, C. G., & Osborne, D. (2021). Examining the relational underpinnings and consequences of system-justifying beliefs: Explaining the palliative effects of system justification. *British Journal of Social Psychology, 60*(3), 1027–1050. https://doi.org/10.1111/bjso.12440

Bahamondes, J., Sibley, C. G., & Osborne, D. (2021). System Justification or Social Dominance? A Multilevel Test of the Ideological Motivators of Perceived Discrimination. *Personality and Social Psychology Bulletin*. https://doi.org/10.1177/01461672211036020

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: theory and cases. *International Relations, 30*(4), 494–531. https://doi.org/10.1177/0047117815596590

Barker, R. (2009). King John's Christmas cards: self-legitimation. In *Legitimating Identities*. https://doi.org/10.1017/cbo9780511490163.003

Baryla, W., Wojciszke, B., & Cichocka, A. (2015). Legitimization and delegitimization of social hierarchy. *Social Psychological and Personality Science, 6*(6), 197–206.

Bates, J. M. (2004). From state monopoly to a free market of ideas? Censorship in Poland, 1976-1989. *Critical Studies, 22*, 141-168.

Baumeister, R. F., & Leary, M. R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin, 117*(3), 497–529. DOI: 10.1037/0033-2909.117.3.497.

Baysal, B. (2020). 20 years of securitization: Strengths, limitations and a new dual framework. *Uluslararasi Iliskiler, 17*(67), 3–20. https://doi.org/10.33458/uidergisi.777338

Beattie, A. (2018, May 13). Data protectionism: The growing menace to global business. Retrieved December 10, 2022, from https://www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb

Berlin, L. N. (2020). *Position and stance in political discourse: The individual, the party, and the party line*. Vernon Press.

Bexell, M., Jonsson, K., & Uhlin, A. (2022). The politics of legitimation and delegitimation in global governance. In M. Bexell, K. Jonsson, & A. Uhlin (Eds.), *Legitimation and Delegitimation in Global Governance*. Oxford University Press.

Biber, D., & Finegan, E. (1988). Adverbial stance types in English. *Discourse Processes, 11*(1), 1–34.

Biber, D., Johansson, S., Leech, G. N., Conrad, S., & Finegan, E. (2021). *Grammar of spoken and written English*. John Benjamins Publishing Company.

Biddle, S. (2020). Facebook Lets Vietnam's Cyberarmy Target Dissidents, Rejecting A Celebrity's Plea, The Intercept, 22 December 2020, https://theintercept.com/2020/12/21/facebook- vietnam-censorship;

Blair, I. V., Judd, C. M., & Fallman, J. L. (2004). The automaticity of race and Af- rocentric facial features in social judgments. *Journal of Personality and Social Psychology, 87*, 763–778.

Blanchar, J. C., & Eidelman, S. (2013). Perceived system longevity increases system justification and the legitimacy of inequality. *European Journal of Social Psychology, 43*, 238–245. http://dx.doi.org/ 10.1002/ejsp.1960

Blasi, G., & Jost, J. T. (2012). System Justification Theory and Research: Implications for Law, Legal Advocacy, and Social Justice. *Ideology, Psychology, and Law*. https://doi.org/10.1093/acprof:oso/9780199737512.003.0003

Blommaert, J., Collins, J., & Heller, M. (2001). Discourse and critique: Part one. *Critique of Anthropology,21,* 5–12.

Boholm, M. (2021). Twenty-five years of cyber threats in the news: A study of Swedish newspaper coverage (1995-2019). *Journal of Cybersecurity,* 1–23.

Bois, J. W. Du. (2007). The stance triangle. In R. Englebretson (Ed.), *Stancetaking in Discourse* (p. 140). https://doi.org/10.1111/j.1467-9841.2010.00447_1.x

Boer, L. J. M., Lodder, A. R. (2012). Cyberwar: What Law to Apply? And to Whom?, W: R. Leukfeldt, W. Stol (eds.), *Cyber Safety: An Introduction*, The Hague: Eleven international publishing.

Bowman-Grieve, L. (2015). Cyber-terrorism and moral panics: A reflection on the discourse of cyberterrorism. In T. Chen, L. Jarvis, & S. Macdonald (Eds.), *Terrorism Online: Politics, Law and Technology* (pp. 86-106). Abingdon: Routledge.

Bradshaw, S. & Howard, P. (2017). Troops, trolls and troublemakers: a global inventory of organ- ized social media manipulation. In: Woolley S and Howard P (eds) *Project on Computational Propaganda*. Oxford: Oxford Internet Institute.

Brandt, M. J. (2013). Do the disadvantaged legitimize the social system? A large-scale test of the status-legitimacy hypothesis. *Journal of Personality and Social Psychology, 104*, 765-785. doi: 10.1037/a0031751

Branscombe, N. R., Ellemers, N., Spears, R., & Doosje, B. (1999). The context and content of social identity threat. In N. Ellemers, R. Spears, & B. Doosje (Eds.), *Social identity: Context, commitment, content* (pp. 35–58). Blackwell Science.

Brito, J., & Watkins, T. (2011). Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. *National Security Journal, 3*(1), 39–84.

Brown, D. (2015). Vietnam's Communists Conjure with the Internet, in: Asia Sentinel, 3 March, online: <www.asiasentinel.com/politics/ vietnam-communists-conjure-internet/>

Bui, N. S., & Lee, J. (2022). Comparative Cybersecurity Law in Socialist Asia. *Vanderbilt Journal of Transnational Law*, *55*(631).

Bui, N. S. (2022). Vietnam's Mixed Constitution and Human Rights. *Law & Ethics of Human Rights, 16*(2), 295–321.

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

Bui, T. H. (2016). The influence of social media in Vietnam's elite politics. *Journal of Current Southeast Asian Affairs, 35*(2), 89–111. https://doi.org/10.1177/186810341603500204

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A New Framework for Analysis*. Colorado & London: Lynne Rienner Publishers.

Cain, G. (2014). Kill One to Warn One Hundred: The Politics of Press Censorship in Vietnam. *International Journal of Press/Politics*, *19*(1), 85–107. https://doi.org/10.1177/1940161213508814

Cankaoxiaoxi. (2011). China, Russia vs. U.S. EU: Struggle for Cyberspace Preeminence. Retrieved August 3, 2022, from http://world.cankaoxiaoxicom/2011/1102/4962.shtml

Cao, L., & Qiaoan, R. (2023). Digital populism in an authoritarian context: A discourse analysis of the legitimization of the Belt and Road Initiative by China's party media. The Communication Review, 26(4), 350–389. https://doi.org/10.1080/10714421.2023.2214056

Cap, P. (2017). The Language of Fear, 15–27. https://doi.org/10.1057/978-1-137-59731-1

Caricati, L., & Owuamalam, C. K. (2020). System Justification Among the Disadvantaged: A Triadic Social Stratification Perspective. *Frontiers in Psychology, 11*(January), 1–6. https://doi.org/10.3389/fpsyg.2020.00040

Carpentier, N. (2017). The Discursive-Material Knot: Cyprus in Conflict and Community Media Participation. https://doi.org/10.1177/0725513618787676

Cavelty, M. D. (2007). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. New York: Routledge.

Cavelty, M. D. (2013a). From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse. *International Studies Review, 15*, 105–22.

Cavelty, M. D. (2013b). The (Il)legitimacy of Cybersecurity. An Application of Just Securitization Theory to Cybersecurity based on the Principle of Subsidiarity. *International Studies Review, 15*(1), 105-122.

Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics, 20*(3), 701-718.

Cavelty, M. D. (2019a). Cyber-Security. In Contemporary Security Studies (5th ed.). Oxford University Press.

Cavelty, M. D. (2019b). The Militarisation of Cyber Security as a Source of Global Tension. Strategic Trends 2012. Key Developments in Global Affairs, 103. Retrieved from http://ssrn.com/abstract=2007043

Cavelty, M. D. (2019c). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics, 20*(3), 701-718.

Cavelty, M. D. (2019d). Cyber-Security. In J. P. Burgess (Ed.), *The Routledge Handbook of New Security Studies* (pp. 154-162). London: Routledge.

Cavelty, M. (2019e). Cyber-Security and the Media. In J. P. Burgess (Ed.), *The Routledge Handbook of Media, Conflict and Security* (pp. 154-162). London: Routledge.

Cheng, L., Liu, Y., & Zhao, Y. (2021). Exploring the U.S. institutional discourse about critical information infrastructure protection (CIIP): A corpus-based analysis. *International Journal of Legal Discourse, 6*(2), 323–347. https://doi.org/10.1515/ijld-2021-2058

Cheng, L., Pei, J., & Danesi, M. (2019). A sociosemiotic interpretation of cybersecurity in U.S. legislative discourse. *Social Semiotics, 29*(3), 286–302. https://doi.org/10.1080/10350330.2019.1587843

Chilton, P. (2004). *Analyzing political discourse: Theory and practice*. London: Routledge.

Chovanec, J. (2010). Legitimation through differentiation: Discursive construction of Jacques Le Worm Chirac as an opponent to military action. In Urszula Okulska and Piotr Cap (eds.), *Perspectives in politics and discourse*, 61–82. Amsterdam: Benjamins

Cichocka, A., & Jost, J. T. (2014). Stripped of illusions? Exploring system justification processes in capitalist and post-Communist societies. *International Journal of Psychology, 49*(1), 6–29. https://doi.org/10.1002/ijop.12011

Citrin, J., McClosky, H., Shanks, J. M., & Sniderman, P. (1975). Personal and political sources of political alienation. *British Journal of Political Science, 5*, 1–31. doi:10.1017/S0007123400008024.

Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperColiins.

Clarke, R. A., & Knake, R. (2019). The internet freedom league. How to push back against the authoritarian assault on the web. *Foreign Affairs, 98*(5), 184–192.

Cloud, D. S., & Bengali, S. (2020, October 22). Facebook touts free speech. In Vietnam, it's aiding in censorship. Retrieved December 10, 2022, from https://www.latimes.com/world-nation/story/2020-10-22/facebook-censorship-suppress-dissent-vietnam

Conway, M. (2008). The Media and Cyberterrorism: A Study in the Construction of 'Reality'. Available at: http://doras.dcu.ie/2142/1/2008–5.pdf (accessed 5 January 2016).

Công An Nhân Dân. (2008). Sự thật v ề 'tờ báo lậu' Tổ Quốc. Retrieved December 15, 2008, from http://www.congan.com.vn/phong_su_dieu_tra/2008/12/20081205.55165.ca

Công An Nhân Dân. (2009). Nguyễn Khắc Toàn, kẻ vụ lợi bằng việc làm phản dân hại nước. Retrieved July 2, 2009, from http://www.cand.com.vn/vi-VN/binhluan/2009/6/114397.cand

Công Khế, N. (2014). A free press for Vietnam. *The New York Times*, 19 November.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*(10), 13–21. https://doi.org/10.22215/timreview835

Creemers, R. (2023). The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy. *Journal of Contemporary China, 1*(1), https://doi.org/10.1080/10670564.2023.2196508.

Day, M. V., Kay, A. C., Holmes, J. G., & Napier, J. L. (2011). System Justification and the Defense of Committed Relationship Ideology. *Journal of Personality and Social Psychology, 101*(2), 291–306. https://doi.org/10.1037/a0023197

Debrix, F. (2001). Cyberterror and media-induced fears: The production of emergency culture. *Strategies: Journal of Theory, Culture & Politics, 14*(1), 149-168.

Deibert, R. J., Palfrey, J. G., Rohozinski, R. and Zittrain, J. (2008) *The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). *Access contested: Security, identity, and resistance in Asian cyberspace*. Cambridge, MA: The MIT Press.

DeScioli, P., & Kurzban, R. (2013). A solution to the mysteries of morality. *Psychological bulletin, 139*(2), 477.

Diamond, J. (1996). *Status and power in verbal interaction*. Amsterdam: John Benjamins Publishing Company.

Dodds, F. & Pippard, T. (2013). *Human and Environmental Security: An Agenda for Change*. London: Earthscan.

Do, T., & Ngo, H. Q. (2023). Patriotism: The Philosophical Foundation of the Vietnamese People and its Manifestations in the Rural Villages. *ISVS E-Journal, 10*(4), 119–133.

Duckett, D. G., Lorenzo-Arribas, A., Horgan, G., et al. (2020). Amplification without the event: the rise of the flexitarian. *Journal of Risk Research*. doi: https://doi.org/10.1080/13669877.2020.1800066

Dukalskis, A., & Patane, C. (2019). Justifying power: When autocracies talk about themselves and their opponents. *Contemporary Politics, 25*(4), 457-478.

Dukalskis, A., & Gerschewski, J. (2017). What autocracies say (and what citizens hear): proposing four mechanisms of autocratic legitimation. *Contemporary Politics, 23*(3), 251-268.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review, 15*(1), 105–122. https://doi.org/10.1111/misr.12023

Dung, P. X., & Ho, B. T. E. (2022). How regime legitimation influences Vietnam's strategy toward US–China strategic rivalry. *International Journal of Asian Studies*, 1–20. https://doi.org/10.1017/s1479591422000286

Dupont, B. (2013). The proliferation of cyber security strategies and their implications for privacy. In K. Benyekhlef & E. Mitjans (Eds.), *Circulation internationale de l'information et sécurité* (pp. 67–80). Montréal: Les Éditions Thémis.

Echterhoff, G., Higgins, E. T., & Levine, J. M. (2009). Shared Reality: Experiencing Commonality with others' Inner States about the World. *Perspectives on Psychological Science, 4*(5), 496–521. https://doi.org/10.1111/j.1745-6924.2009.01161.x

Edel, M., & Josua, M. (2018). How authoritarian rulers seek to legitimize repression: framing mass killings in Egypt and Uzbekistan. *Democratization*, *25*(5), 882–900. https://doi.org/10.1080/13510347.2018.1439021

Eidelman, S., & Crandall, C. S. (2012). Bias in favor of the status quo. *Social and Personality Psychology Compass, 6*(3), 270–281. https://doi.org/10.1111/j.1751-9004.2012.00427.x

Emerson, R. M. (1962). Power-Dependence Relations. *American Sociological Review, 27*(1), 31–41. https://doi.org/10.2307/2089716

Eriksson, J. (2001). Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management, 9*(3), 211-222.

Fairclough, N. (1995). *Media discourse*. London: Edward Arnold.

Fforde, A., & Homutova, L. (2017). Political authority in Vietnam: Is the Vietnamese communist party a paper Leviathan? *Journal of Current Southeast Asian Affairs, 36*(3), 91–118. https://doi.org/10.1177/186810341703600304

Fichtner, L., Pieters, W., & Teixeira, A. (2016). Cybersecurity as a Politikum: Implications of security discourses for infrastructures. ACM International Conference Proceeding Series, 26-29-Sept, 36–48. https://doi.org/10.1145/3011883.3011887

Flowerdew, L. (2012). Corpus-based discourse analysis. In J. P. Gee & M. Handford (Eds.), *Routledge Handbook of Discourse Analysis*. Routledge.

Freud. (1946). *The Ego and A4echanisms of Defense*. New York: International University Press.

Friesen, J. P., Laurin, K., Shepherd, S., Gaucher, D., & Kay, A. C. (2019). System justification: Experimental evidence, its contextual nature, and implications for social change. *British Journal of Social Psychology, 58*(2), 315–339. https://doi.org/10.1111/bjso.12278

Froschauer, U. M. (2016). *The Wedding Performance: Gender Performance and System Justification in the White Wedding*. University of KwaZulu-Natal.

Gablasova, D. (2021). Examining Vocabulary Acquisition Through Word Associations Triangulating the Psycholinguistic and Corpus-Based Approaches. In K. Wu, *Using Corpus Methods to Triangulate Linguistic Analysis* (pp. 141-162). New York: Routledge.

Geddes, B. (1999). What do we know about democratization after twenty years? *Annual Review of Political Science, 2*, 115-144.

Geis, F. L. (1993). Self- fulfilling prophecies: A social psychological view of gender. In A. E. Beall & R. J. Sternberg (Eds.), *Perspectives on the psychology of gender* (pp. 9–54). New York: Guilford.

Gidda. (2019). China's New Cybersecurity Law Sparks Fresh Censorship and Espionage Fears.

Gillespie, J. (2016). Public Discourse and Constitutional Change: A Comparison of Vietnam and Indonesia. *Asian Journal of Comparative Law, 11*(2), 209–218. https://doi.org/10.1017/asjcl.2016.17

Górka, M. (2021). Cybersecurity Politics – Conceptualization of the Idea. *Polish Political Science Yearbook, 50*(June), 1–19. https://doi.org/10.15804/ppsy202112

Górka, M. (2023). Conceptualising securitisation in the field of cyber security policy. *Journal of Modern Science, 53*(4), 263–290. https://doi.org/10.13166/jms/176103

Grobler, M., Gaire, R., & Nepal, S. (2021). *Frontiers in Big Data, 4*(March), 1–18. https://doi.org/10.3389/fdata.2021.583723

Gutierrez, R., & Giner-Sorolla, R. (2007). Anger, disgust, and presumption of harm as reactions to taboo-breaking behaviors. *Emotion, 7*, 853-868. doi:10.1037/1528-3542.7.4.853

Haack, P., & Sieweke, J. (2018). The Legitimacy of Inequality: Integrating the Perspectives of System Justification and Social Judgment. *Journal of Management Studies, 55*(3), 486–516. https://doi.org/10.1111/joms.12323

Haines, E. L., & Jost, J. T. (2000). Placating the powerless: Effects of legitimate and illegitimate explanation on affect, memory, and stereotyping. *Social Justice Research, 13*(3), 219–236. https://doi.org/10.1023/A:1026481205719

Hama, H. H. (2017). State Security, Societal Security, and Human Security. *Journal of International Relations, 21*(1), 1–19. https://doi.org/10.1177/0973598417706591

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*, 1155–1175.

Hardin, C. D., & Conley, T. D. (2001). A relational approach to cognition: Shared experience and relationship affirmation in social cognition. In G. B. Mosko- witz (Ed.), *Cognitive social psychology: The Princeton symposium on the legacy and future of social cognition* (pp. 3-17). Mahwah, NJ: Erlbaum

Hassib, B., & Shires, J. (2021). Manipulating uncertainty: Cybersecurity politics in Egypt. *Journal of Cybersecurity, 7*(1), 1–16. https://doi.org/10.1093/cybsec/tyaa026

Hennes, E. P., Nam, H. H., Stern, C., & Jost, J. T. (2012). Not all ideologies are created equal: Epistemic, existential, and relational needs predict system-justifying attitudes. *Social Cognition, 30*, 669-688.

Hersee, S. (2019). *The Cyber Security Dilemma And The Securitisation Of Cyberspace*.

University of London.

Hilton, K., Siami Namin, A., & Jones, K. S. (2022). Metaphor identification in cybersecurity texts: a lightweight linguistic approach. *SN Applied Sciences, 4*(2). https://doi.org/10.1007/s42452-022-04939-8

Higgins, E.T. (1996). Knowledge activation: Accessibility, applica- bility, and salience. In E.T. Higgins & A.W. Kruglanski (Eds.), *Social psychology: Handbook of basic principles* (pp. 133–168). New York: Guilford.

Hookway, J. (2017). Introducing Force 47, Vietnam's New Weapon AgainstOnline Dissent, Wall Street Journal, 31 December 2017, https://www.wsj. com/articles/introducing-force-47-vietnams-new-weapon-against-online- dissent-1514721606

Holst, J., & van de Pas, R. (2023). The biomedical securitization of global health. *Globalization and Health, 19*(1), 1–9. https://doi.org/10.1186/s12992-023-00915-y

Hung, M. (2018). Luật An ninh mạng phù hợp với Hiến pháp, không cản trở thực hiện các điều ước quốc tế mà Việt Nam là thành viên. Communist Party of Vietnam Online Newspaper. Retrieved from https://dangcongsan.vn/thoi-su/luat-an-ninh-mang-phu-hop-voi-hien-phap-khong-can-tro-thuc-hien-cac-dieu-uoc-quoc-te-ma-viet-nam-la-thanh-vien-487399.html

Hunston, S., & Sinclair, J. (2000). A local grammar of evaluation. In S. Hunston & G. Thompson (Eds.), *Evaluation in Text: Authorial Stance and The Construction of Discourse* (pp. 74–101). New York: Oxford University Press.

Huysmans, J. (2006). The Politics of Insecurity: Fear, Migration and Asylum in the EU. London: Routledge.

Huysmans, J. (2008). The jargon of exception – on Schmitt, Agamben and the absence of political society. *International Political Sociology, 2*(2), 165–183.

Jamil, H., Zia, T., Nayeem, T., Whitty, M. T., & D'Alessandro, S. (2024). Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. *Information and Computer Security, ahead-of-print*. https://doi.org/10.1108/ICS-10-2023-0176

Jarvis, L., Macdonald, S., & Whiting, A. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. European *Journal of International Security, 2*(1), 64–87. https://doi.org/10.1017/eis.2016.14

Jarvis, L., Macdonald, S., & Whiting, A. (2015). Constructing cyberterrorism as a security threat: A study of international news media coverage. *Perspectives on Terrorism, 9*(1), 60-75.

Jaskulowski, K. (2019). The securitisation of migration: Its limits and consequences. International Political Science Review, 40(5), 710–720. https://doi.org/10.1177/0192512118799755

Jebe, R., Mayer, D., & Lee, Y.-S. (2012). China's Export Restrictions of Raw Materials and Rare Earths: A New Balance Between Free Trade and Environmental Protection?. *Geo. Wash. Int'l L. Rev., 44*, 579-630.

Jolley, D., Douglas, K. M., & Sutton, R. M. (2018). Blaming a few bad apples to save a threatened barrel: The system-justifying function of conspiracy theories. *Political Psychology, 39*, 465– 478. https://doi.org/10.1111/pops.12404

Jones, J. J. G. (2022). Hostile Forces How the Chinese Communist Party Resists International Pressure on Human Rights.

Jost, J. T., & Banaji, M. R. (1994). The role of stereotyping in system justification and the production of false consciousness. *British Journal of Social Psychology, 33*(1), 1–27. https://doi.org/10.1111/j.2044-8309.1994.tb01008.x

Jost, J. T., Pelham, B.W., Sheldon, O., & Sullivan, B. N. (2003). Social inequality and the reduction of ideological dissonance on behalf of the system: Evidence of enhanced system justification among the disadvantaged. *European Journal of Social Psychology, 33*, 13–36.

Jost, J. T., Banaji, M. R., & Nosek, B. A. (2004). A Decade of System Justification Theory: Accumulated Evidence of Conscious and Unconscious Bolstering of the Status Quo. *Political Psychology, 25*(6), 881–919. https://doi.org/10.1111/j.1467-9221.2004.00402.x

Jost, J. T., Ledgerwood, A., & Hardin, C. D. (2008). Shared Reality, System Justification, and the Relational Basis of Ideological Beliefs. *Social and Personality Psychology Compass, 2*(1), 171–186. https://doi.org/10.1111/j.1751-9004.2007.00056.x

Jost, J. T., Kay, A. C., & Thorisdottir, H. (2009). *Social and Psychological Bases of Ideology and System Justification*. Oxford University Press.

Jost, J. T., Chaikalis-Petritsis, V., Abrams, D., Sidanius, J., van der Toorn, J., & Bratt, C. (2012). Why men (and women) do and don't rebel: Effects of system justification on willingness to protest. *Personality and Social Psychology Bulletin, 38*(2), 197–208. https://doi.org/10.1177/0146167211422544

Jost, J. T., & van der Toorn, J. (2012). System justification theory. In P. A. M. van Lange, A. W. Kruglanski, & E. T. Higgins (Eds.), *Handbook oftheories ofsocial psychology* (Vol. 2, pp. 313–343). London, England: Sage.

Jost, J. T., Langer, M., Badaan, V., Azevedo, F., Etchezahar, E., Ungaretti, J., & Hennes, E. P. (2017). Ideology and the limits of self-interest: System justification motivation and conservative advantages in mass politics. *Translational Issues in Psychological Science*, *3*(3), e1–e26. https://doi.org/10.1037/tps0000127

Jost, J. T. (2019). A quarter century of system justification theory: Questions, answers, criticisms, and societal applications. *British Journal of Social Psychology, 58*(2), 263–314. https://doi.org/10.1111/bjso.12297

JOST, J. T. (2020a). A New "Discourse of Voluntary Servitude." *A Theory of System Justification*, 1–12. https://doi.org/10.2307/j.ctv13qfw6w.4

JOST, J. T. (2020b). Does a Sense of Powerlessness Foster the Legitimation of Authority and Hierarchy? In *A Theory of System Justification* (p. 139). Harvard University Press.

JOST, J. T. (2020c). Intellectual Precursors, Major Postulates, and Practical Relevance of System Justification Theory. In *A Theory of System Justification* (pp. 49–69). https://doi.org/10.3390/su70x000x

Jost, J. T., & Kende, A. (2020). Setting the record straight: System justification and rigidity-of-the-right in contemporary Hungarian politics. *International Journal of Psychology*, *55*(S1), 96–115. https://doi.org/10.1002/ijop.12631

Kay, A. C., & Jost, J. T. (2003). Complementary Justice: Effects of "Poor but Happy" and "Poor but Honest" Stereotype Exemplars on System Justification and Implicit Activation of the Justice Motive. *Journal of Personality and Social Psychology, 85*(5), 823–837.

https://doi.org/10.1037/0022-3514.85.5.823

Kay, A. C., Jost, J. T., & Young, S. (2005). Victim derogation and victim enhancement as alternate routes to system justification. *Psychological Science, 16*, 240–246. https://doi.org/10.1111/j. 0956-7976.2005.00810.x

Kay, A. C., Gaucher, D., Napier, J. L., Callan, M. J., & Laurin, K. (2008). God and the government: Testing a compensatory control mechanism for the support of external systems of control. *Journal of Personality and Social Psychology, 95*,18–35.

Kay, A. C., Gaucher, D., Peach, J. M., Laurin, K., Friesen, J., Zanna, M. P., & Spencer, S. J. (2009). Inequality, discrimination, and the power of the status quo: Direct evidence for a motivation to see the way things are as the way they should be. *Journal of Personality and Social Psychology, 97*, 421-434.

Kawakami, K., Dovidio, J. F., & Dijksterhuis, A. (2003). Effect of social category priming on personal attitudes. *Psychological Science, 14*, 315–319.

Keller, P. (1994). Sources of Order in Chinese Law. *Am. J. Comp. L., 42,* 711-749.

Kelemen, L., Szabó, Z. P., Mészáros, N. Z., László, J., & Forgas, J. P. (2014). Social cognition and democracy: The relationship between system justification, just world beliefs, authoritarianism, need for closure, and need for cognition in Hungary. Journal of Social and Political Psychology, 2(1), 197–219. https://doi.org/10.5964/jspp.v2i1.208

Kennedy, G. (2001). Corpus linguistics. In N. J. Smelser & P. B. B. Baltes (Eds.), *International encyclopedia of the social & behavioral sciences* (pp. 30556-30562). Pergamon. https://www.sciencedirect.com/science/article/pii/B0080430767030564

Kerr, P. 2010. 'Human Security', in A. Collins, ed., *Contemporary Security Studies* (pp. 121–135). New York, NY: Oxford University Press.

Klein, J., & Hossain, K. (2020). Conceptualising Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change. *Arctic Review on Law and Politics, 11*(0), 1. https://doi.org/10.23865/arctic.v11.1936

Kiem Sat Online. (2020, January 13). "Tự do ngôn luận" hay "ngôn luận tự do" để xuyên tạc, kích động chống phá Đảng, Nhà nước và nhân dân. Retrieved December 10, 2022, from

https://kiemsat.vn/tu-do-ngon-luan-hay-ngon-luan-tu-do-de-xuyen-tac-kich-dong-chong-pha-dang-nha-nuoc-va-nhan-dan-56473.html

Kingdon, J. W. (2003). *Agendas, Alternatives, and Public Policies* (2nd ed.). New York: Harper Collins College Publishers.

Kneuer, M. Legitimation beyond ideology: authoritarian regimes and the construction of missions. *Z Vgl Polit Wiss 11*, 181–211 (2017). https://doi.org/10.1007/s12286-017-0335-z

Kopylec, J., D'Amico, A., & Goodall, J. (2008). Visualizing cascading failures in critical cyber infrastructures. *IFIP Advances in Information and Communication Technology, 253*, 351–364.

Kovacs, A., & Hawtin, D. (2013). Cyber Security, Cyber Surveillance and Online Human Rights. In *Stockholm Internet Forum on Internet Freedom for Global Development*. Global Partners & Associates, Stockholm.

Krauss, R. M., & Deutsch, M. (1966). Communication in interpersonal bargaining. *Journal of Personality and Social Psychology, 4*(5), 572–577. https://doi.org/10.1037/h0023899

Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information and Communications Technology Law, 23*(3), 220–237. https://doi.org/10.1080/13600834.2014.970432

Kruglanski, A.W. (2004). *The psychology of closed mindedness*. New York: Psychology Press.

Kübler, S., & Zinsmeister, H. (2015). *Corpus linguistics and linguistically annotated corpora*. Bloomsbury Academic.

Kumar, S. (2021). The missing piece in human-centric approaches to cybernorms implementation: the role of civil society. *Journal of Cyber Policy, 6*(3), 375–393. https://doi.org/10.1080/23738871.2021.1909090

Kyrgos, Z. S., & Pantazis, D. G. (2021). Health and Migration: Health Securitization and Policy-Making Perspectives in the Post-Pandemic Era. *HAPSc Policy Briefs Series, 2*(1), 118. https://doi.org/10.12681/hapscpbs.27667

Kyzym, A. (2021). *Autocratic Legitimation: A Hierarchical Cluster Analysis of Authoritarian Rulers ' Claims To Legitimacy*. https://doi.org/10.13140/RG.2.2.21195.52001

Labov, W., & Waletzky, J. (1967). Narrative analysis: Oral version of personal experience. In Helm (Ed.), Essays on the verbal and visual arts: Proceedings of the 1966 Annual Spring Meeting of the American Ethnological Society (pp. 12-44). Seattle: University of Washington Press.

Lam, V. (2022). Information and Communications Technologies, Online Activism, and Implications for Vietnam's Public Diplomacy. *Journal of Current Southeast Asian Affairs, 41*(1), 3–33. https://doi.org/10.1177/18681034211002850

Lawson, S. (2011). Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History. In *Beyond Cyber-Doom*.

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. J*ournal of Information Technology & Politics, 10*, 86–103. doi:10.1080/19331681.2012.759059

Lawson, S., & Middleton, M. K. (2019, March 4). Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016. First Monday, 24(3). Retrieved from https://firstmonday.org/ojs/index.php/fm/article/view/9623/7736

Laurin, K., Kay, A. C., & Fitzsimons, G. J. (2012). Reactance versus rationalization: Divergent responses to policies that constrain freedom. *Psychological Science, 23*, 205–209. https://doi. org/10.1177/0956797611429468

Lee, I. (2018). The Power of Ambivalence: Using Ambivalence as a Healing Resource for Asian Women in the Confucian Context. *Pastoral Psychology*, *67*(4), 373–387. https://doi.org/10.1007/s11089-018-0820-6

Le, H. H. (2012). Performance-based legitimacy: The case of the communist party of Vietnam and doi moi. *Contemporary Southeast Asia*, *34*(2), 145–172. https://doi.org/10.1355/cs34-2a

Le. H., H. (2019). The Political Economy of Growth in Vietnam. *ISEAS Perspective*, (77), 1–7. https://doi.org/10.4324/9780429321375

Le Kien, 2018. Tiếp xúc cử tri, Tổng bí thư phát biểu v`ềcác vụ biểu tình, gây rối. [Online] Available at: https://tuoitre.vn/tiep-xuc-cu-tri-tong-bi-thu-phat-bieu-ve-cac-vu-bieu-tinh-gay-roi- 20180617113154864.htm [Accessed 26 September 2022].

Léonard, S., & Kaunert, C. (2011). Reconceptualizing the Audience in Securitization Theory. In T. Balzacq (Ed.), *Securitization Theory: How Security Problems Emerge and Dissolve* (pp. 1-20). London: Routledge.

Le, V.-T., Nguyen, P.-L., & Ngo, Q.-D. (2020). Cybersecurity Maintenance in Vietnam in 4.0 Era. People Security's Academy of VietNam.

Levy, S. R., West, T. L., Ramirez, L., & Karafantis, D. M. (2006). The Protestant work ethic: A lay theory with dual intergroup implications. Group Processes & Intergroup Relations, 9, 95–115. doi:10.1177/ 1368430206059874

Lesmana, T. (2016). Freedom of the Press in Vietnam and Laos: Fred Siebert's Communist Media Theory Re-Examined. Daniel K. Inouye Asia-Pacific Center for Security Studies, 31.

Leeuwen, T. van. (2008). *Discourse and Practice: New Tools for Critical Discourse Analysis*.

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the Current Literature: A Reference Framework. *Computers in Industry, 103*(1), 97-110.

Liaropoulos, A. N. (2016). Reconceptualising Cyber Security. *International Journal of Cyber Warfare and Terrorism, 6*(2), 32–40. https://doi.org/10.4018/ijcwt.2016040103

Lindsay, J. (2014). The Impact of China on Cybersecurity: Fiction and Friction. *International Security, 39*(3), 7-47.

Lind, E. A. & Tyler, T. R. (1988). *The Social Psychology of Procedural Justice*. New York: Plenum Press.

Lindvall, E. (2020). *More Dangerous than Guns and Tanks: How Cybersecurity Is Framed by the EU and Sweden*. Uppsala University.

Li, W., Yang, Y., Wu, J., & Kou, Y. (2020). Testing the Status-Legitimacy Hypothesis in China: Objective and Subjective Socioeconomic Status Divergently Predict System Justification.

Personality and Social Psychology Bulletin, 46(7), 1044–1058. https://doi.org/10.1177/0146167219893997

Liaropoulos, A. (2012). A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia. *Information Warfare, 4*(January), 1–330. https://doi.org/10.1002/9781118381533

Lim, G. (2020). Securitize/Counter-Securitize: The Life and Death of Malaysia's Anti-Fake News Act.

Linell, P. (1998). *Approaching dialogue: Talk, interaction and contexts in dialogical perspective*. Amsterdam/Philadelphia: John Benjamins.

Lindsay, J. (2014). The Impact of China on Cybersecurity: Fiction and Friction. *International Security, 39*(3), 7–47.

Lobo-Guerrero, L. (2008). 'Pirates', stewards, and the securitization of global circulation. *International Political Sociology, 2*, 219–235.

Long, T. Van. (2020). Realizing the barrier to the practice of e-democracy in Vietnam. *PalArch's Journal of Archaeology of Egypt, 17*(3), 1–15. Retrieved from https://www.archives.palarch.nl/index.php/jae/article/view/91

Lönnqvist, J. E., Szabó, Z. P., & Kelemen, L. (2021). "The New State That We Are Building": Authoritarianism and System-Justification in an Illiberal Democracy. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.703280

Luiijf, H. A. M., Besseling, K., Spoelstra, M., & De Graaf, P. (2013). Ten national cyber security strategies: A comparison. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6983 LNCS(January), 1–17. https://doi.org/10.1007/978-3-642-41476-3_1

Luong, D. N. A. (2022). A Study Of Vietnam's Control Over Online Anti-State Content.

Macek, P., & Markova, I. (2004). Trust and distrust in old and new democracies. In I. Markova (Ed.), *Trust and democratic transition in post-communist Europe* (pp. 173–193). New York, NY: Oxford University Press

MacKinnon, C. A. (1989). *Towarda Feminist Theory of the State*. Cambridge, MA: Harvard University Press.

McKinley, C. (2008) Can a state-owned media effectively monitor corruption? A study of Vietnam's printed press. *Asian Journal of Public Affairs* 2(1): 12–38.

Mai, T. T. (2019). *The Politics of Nationalism in the Vietnamese Communist Discourse* (PhD Thesis). University of Bristol.

Magee, J. C., & Galinsky, A. D. (2008). Social hierarchy: The self-reinforcing nature of power and status. *The Academy of Management Annals, 2* , 351–398.

Mello, J. P. (2020, October 1). Cyberwarfare report, Vol 5, No. 3: U.S Election security threats and warnings. Retrieved from https://cybersecurityventures.com/cyberwarfare-report-q4-2020-u-s-election-security-threats-and-warnings/

Miao, W., & Han, R. (2021). Modernization Planner, Authoritarian Paternalist, and Rising Power: Evolving Government Positions in China's Internet Securitization. *Journal of Contemporary China, 31*(136), 574–591. https://doi.org/10.1080/10670564.2021.1985832

Miao, W., Xu, J., & Zhu, H. (2020). From Technological Issue to Military-Diplomatic Affairs: Analysis of China's Official Cybersecurity Discourse (1994–2016). Second International Handbook of Internet Research, 431–443. https://doi.org/10.1007/978-94-024-1555-1_61

Mishra, N. (2020). The trade: (cyber)security dilemma and its impact on global cybersecurity governance. *Journal of World Trade, 54*(4), 567–590. https://doi.org/10.54648/trad2020025

Murray, R. A. (2015). System justification, work ethic, and just-world beliefs: A motivated reasoning perspective. *The Sciences and Engineering, 75*(10). Retrieved from http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=psyc12&NEWS=N&AN=2015-99080-397

Neo, R. (2022). When Would a State Crack Down on Fake News? Explaining Variation in the Governance of Fake News in Asia-Pacific. *Political Studies Review, 20*(3), 390–409. https://doi.org/10.1177/14789299211013984

Nguyen-Thu, G. (2018). Vietnamese media going social: Connectivism, collectivism, and conservatism. *Journal of Asian Studies, 77*, 895-918.

Nguyen, H. N. (2022). Regulating Cyberspace in Vietnam: Entry, Struggle, and Gain. *Columbia Journal of Asian Law, 35*(2), 160–199. https://doi.org/10.52214/cjal.v35i2.10028

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*, 1–18. https://doi.org/10.1093/jhuman/huac007

Nguyen, M. QMN. (2023). Media presentations of Vietnam's cybersecurity law: A comparative approach with corpus-based critical discourse analysis. *Computer Law and Security Review*, *50*, Article 105835. https://doi.org/10.1016/j.clsr.2023.105835

Nicimbikije, G. (2020). Speech over! Securitization in acts: National economic security. *International Journal of Political Science and Governance, 2(*1), 24–30. https://doi.org/10.33545/26646021.2020.v2.i1a.29

Nikkei Asia. (2018). Vietnam's cybersecurity law sparks concerns from businesses. Retrieved from https://asia.nikkei.com/Politics/Vietnam-s-cybersecurity-law-sparks-concerns-from-businesses

Nyman, J., & Zeng, J. (2016). Securitization in Chinese climate and energy politics. *Wiley Interdisciplinary Reviews: Climate Change, 7*(2), 301–313.

OpenNet Initiative. (2005). Internet filtering in China in 2004–2005: A country study. Retrieved May, 28, 2007. https://opennet.net/countries/china

Owiny, M. (2022). Advancing a Human-centric approach to cybersecurity policy making. Center for Multilateral Affairs. https://thecfma.org/advancing-a-human-centric-approach-to-cybersecurity-policy-making/

Owuamalam, C. (2018). Do the Disadvantaged Support Social Systems? A Critical Review of the (Un)conscious Basis for System Attitudes Amongst the Disadvantaged. *Social and Personality Psychology Compass, 12*(11).

Palaniappan, M. (2022). *Cyber Sovereignty: In Search of Definitions, Exploring Implications*. Observer Research Foundation.

Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity, 4*(1). https://doi.org/10.1186/s42400-021-00071-z

Panetta, L. (2012). Defending the Nation From Cyber Attacks. Presentation to Business Executives for National Security, New York, NY, 2 October 2012.

Pavlova, P. (2020). Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups. *Peace Human Rights Governance, 4*(3). https://doi.org/10.14658/pupj-phrg-2020-3-4

Phan, L. (2021). Cybersecurity in a one-party state: Policies and implications for Vietnam's economy and online freedom. In S. N. Romaniuk & M. Manjikian (Eds.), *Companion to Global Cyber-Security Strategy* (pp. 297-314). New York: Routledge.

Philo, G. (2007). Can Discourse Analysis Successfully Explain the Content of Media and Journalistic Practice? *Journalism Studies, 8*(2): 175-196.

Philpott, D. (2020). Sovereignty. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Fall 2020). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/fall2020/entries/sovereignty/

Pytlak, A. (2023. Exploring human-centric cybersecurity. Humanitarian Disarment. https://humanitariandisarmament.org/2023/02/06/exploring-human-centric-cyber-security/

Quân Đội Nhân Dân. (2007). Internal-external collusion and insidious political plots. Retrieved September 7, 2007, from http://www.qdnd.vn/qdnd/baongay.quocphong.anninh.22783.qdnd

Quang, T. D. (n.d.). Tăng cường công tác an toàn, an ninh mạng trong tình hình mới. Vietnam Government Portals. Retrieved from http://baochinhphu.vn/Hoat-dong-cua-lanh-dao-Dang-Nha- nuoc/Tang-cuong-cong-tac-bao-dam-an-toan-an-ninh-mang-trong-tinh-hinh-moi/314458.vgp (accessed date).

Quinn, J. (2017). A peek over the great firewall: A breakdown of China's new cybersecurity law. *Science and Technology Law Review, 20*(2), 407-425. https://scholar.smu.edu/scitech/vol20/iss2/18

Radkiewicz, P. (2007). Several reasons why social anomie and political alienation may influence ethnocentric attitudes: The compensating role of authoritarian-paranoid beliefs. *Polish Psychological Bulletin, 38*, 5–14.

Reyes, A. (2011). Strategies of legitimization in political discourse: From words to actions.

Discourse and Society, 22(6), 781–807.

Rid, T. (2013). *Cyberwar Will Not Take Place*. London: Hurst.

Romaine, S. (2000). *Language in society: An introduction to sociolinguistics*. Oxford University Press.

Ross, C., & Ross, L. (1997). *Language and Law: Sources of Systemic Vagueness and Ambiguous Authority in Chinese Statutory Language*. U. Brit. Colum. L. Rev., 31, 205-209.

Rozin, P., Markwith, M., & Stoess, C. (1997). Moralization and becoming a vegetarian: The transformation of preferences into values and the recruitment of disgust. *Psychological Science, 8*, 67-73. doi:10.1111/j.1467-9280.1997.tb00685.x

Sallinen, M. (2020). Weaponized Malware, Physical Damage, Zero Casualties – What Informal Norms Are Emerging in Targeted State Sponsored Cyber-Attacks?

Samson, K. (2018). Trust as a mechanism of system justification. *PLoS ONE*, *13*(10), 1–22. https://doi.org/10.1371/journal.pone.0205566

Sanko, C. (2016). New wine in an old bottle? Anniversary journalism and the public commemoration of the end of the war in Vietnam. *Global Media Journal: German Edition* 6(2).

Savenet (2019). Facts about Cyber Security Law. Hanoi: SaveNet.

Schmitt, C. (2007). The concept of the political. In G. Schwab (Ed.), *The concept of the political* (pp. 19–79). University of Chicago Press.

SCMP. (2019). New year, new repression: Vietnam imposes draconian 'China-like' cybersecurity law. Retrieved from https://www-scmp-com.eu1.proxy.openathens.net/news/asia/southeast-asia/article/2180263/new-year-new-repression-vietnam-imposes-draconian-china (accessed December 10, 2022).

Segal, A., Akimenko, V., Giles, K., Pinkston, D. A., Lewis, J. A., Bartlett, B., … Noor, E. (2020). The Future of Cybersecurity across the Asia-Pacific. *Asia Policy*, *15*(2), 57–59.

Sharikov, P. A. (2019). Evolution of American Cyber Security Policies. *Mirovaya Ekonomika i Mezhdunarodnye Otnosheniya, 63*(10), 51-58. http://doi.org/10.20542/0131-2227-2019-63-10-51-58

Sherif, M. (1966). *The psychology of social norms*. Harper Torchbooks.

Sherman, J. (2019). Vietnam's Internet Control: Following in China's Footsteps? The Diplomat. Retrieved from https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/

Shi, X., Wu, J., & Wei, L. (2022). Stance Taking in News Interviews Based on Stance Triangle and Conversational Analysis. *Open Journal of Modern Linguistics, 12*(02), 188–206. https://doi.org/10.4236/ojml.2022.122015

Sinclair, J.McH. (2004). *Trust the text*. Routledge.

Shires, J. (2020a). *The politics of cybersecurity in the Middle East*. London: Hurst.

Shires, J. (2020b). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*, *41*(1), 82–107. https://doi.org/10.1080/13523260.2019.1670006

Shockley, E., Wynn, A., & Ashburn-Nardo, L. (2016). Dimensions of Black identity predict system justification. *Journal of Black Psychology, 42*, 103–113. http://dx.doi.org/10.1177/00957984 14557276

Sidanius, J. & Pratto, F (1993). The inevirabiliry ofoppression and the dynamics of social dominance. In P. Sniderman & P. E. Terlock (Edo), Prejudice, Politics, and the American Dilema. Stanford, CA: Stanford University Press.

Sombatpoonsiri, J. (2021). Securitizing “Fake News”: Policy Responses to Disinformation in Thailand. From Grassroots Activism to Disinformation, (Weerawan), 105–125. https://doi.org/10.1355/9789814951036-007

Sowińska, A., & Dubrovskaya, T. (2012). Discursive construction and transformation of ‘us’ and ‘them’ categories in the newspaper coverage on the US anti-ballistic missile system: Polish versus Russian view. *Discourse and Society, 6*(4), 449–468

Stangor, C., Sechrist, G.B., & Jost, J.T. (2001). Changing racial beliefs by provid- ing consensus

information. *Personality and Social Psychology Bulletin, 27*, 486-496.

Stapel, D. A., & Noordewier, M. K. (2011). The mental roots of system justification: System threat, need for structure, and stereotyping. *Social Cognition, 29*(3), 238–254. https://doi.org/10.1521/soco.2011.29.3.238

Stivas, D. (2021). Greece's response to the European refugee crisis: A tale of two securitizations. *Mediterranean Politics, 28*(1). DOI: 10.1080/13629395.2021.1902198

Stritzel, H. (2007). Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations, 13*(3), 357–383.

Sumanth, J. J., Mayer, D. M., & Kay, V. S. (2011). Why good guys finish last: The role of justification motives, cognition, and emotion in predicting retaliation against whistleblowers. *Organizational Psychology Review, 1*(2), 165–184. https://doi.org/10.1177/2041386611398283

Susan, K. (2005). Fear-mongering or fact: The construction of "cyber-terrorism" in U.S., U.K, and Canadian news media. *Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities* (732). https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/susan_keith.pdf (accessed 5 January 2016).

Szabolcs, V. (2002). Hacktivists or cyberterrorists? The changing media discourse on hacking. *First Monday, 7*(10), n.p.

Tai, H. S. (2018). Nhận diện và đập tan những luận điệu xuyên tạc Luật An ninh mạng. Communist Party of Vietnam Online Newspaper. Retrieved from https://dangcongsan.vn/tieu-diem/nhan-dien-va-dap-tan-nhung-luan-dieu-xuyen-tac-luat-an-ninh-mang---489084.html

Tajfel, H., & Turner, J. C. (1986). The social identity theory of intergroup behavior. In S. Worchel & W. G. Austin (Eds.), *The social psychology ofintergroup relations* (pp. 7–24). Chicago, IL: Nelson-Hall.

Takong. (2014). Deputy Director of the National Internet Information Office Talk about the CyberSecurity: Mismanagement Leads the Nation in Peril. Takungpao. Retrieved August 3, 2022, from http://news.takungpao.com/mainland/focus/2014-05/2481785.html

Tay Ninh Online. (2021). Họ đã nói sai sự thật như thế nào? Retrieved from https://baotayninh.vn/ho-da-noi-sai-su-that-nhu-the-nao--a134386.html (accessed December 10, 2022).

Teo, K. X. (2021). Civil Society Responses to Singapore's Online "Fake News" Law. International Journal of Communication, 15, 4795–4815. Retrieved from http://ijoc.org.

Thayer, C. A. (2009a). Political Legitimacy of Vietnam's One PartyState: Challenges and Responses. *Journal of Current Southeast Asian Affairs*, *28*(4), 47–70. https://doi.org/10.1177/186810340902800403

Thayer, C. A. (2009b). Vietnam and the Challenge of Political Civil Society. *Contemporary Southeast Asia*, *31*(1), 1–27. https://doi.org/10.1355/cs31-1a

Thayer, C. A. (2010). Political legitimacy in Vietnam: Challenge and response. *Politics and Policy*, *38*(3), 423–444. https://doi.org/10.1111/j.1747-1346.2010.00242.x

Thayer, C. A. (2020). Vietnam's security in the 21st century: Domestic and international dimensions. ISEAS- Yusof Ishak Institute.

The Routledge handbook of new security studies. (2010). In M. Dunn Cavelty & V. Mauer (Eds.), Routledge handbooks. https://doi.org/10.4324/9780203859483

Thompson, G., & Hunston, S. (2000). Evaluation: An introduction. In S. Hunston & G. Thompson (Eds.), *Evaluation in Text: Authorial Stance and the Construction of Discourse* (pp. 1–27). New York: Oxford University Press.

Tien Thang, 2018. Thủ tướng mong dân tỉnh táo trước những luận điệu xuyên tạc. [Online] Available at: https://tuoitre.vn/thu-tuong-mong-dan-tinh-tao-truoc-nhung-luan-dieu-xuyen-tac- 20180618135426373.htm [Accessed 26 September 2022].

Tikk, E., & Kerttunen, M. (Eds.). (2020). Routledge Handbook of International Cybersecurity. Routledge.

Tileagă, C. (2012). *Public apologia, moral transgression and degradation ceremonies*. Revista De Psihologia Sociala 30: 67–78.

Ton, N. M. N., & Hoang. T. T. H. (2023). Construction of roles, obligations and values in politicians' discourses on anti-corruption. *Cogent Social Sciences, 9*(1), 2249286. https://doi.org/10.1080/23311983.2023.2249286

Törnberg, A., & Törnberg, P. (2016). Muslims in social media discourse: Combining topic modeling and critical discourse analysis. *Discourse, Context and Media, 13*, 132-144. http://dx.doi.org/10.1016/j.dcm.2016.04.003

Trinh, M. H., & Vu, T. A. (2023). Nationalism in discursive legitimation: An analysis of the Vietnamese Communist Party's 'bamboo diplomacy' discourse on digital journalism. *Discourse and Society*. https://doi.org/10.1177/09579265231217063

Truong, M. (2024). Declining opportunities for speaking out: The impact of Vietnam's new leadership on grassroots collective action. *Asian Journal of Comparative Politics*, *9*(1), 50–68. https://doi.org/10.1177/20578911221139764

Truong Thuy, T. (2000). *Vietnam's Relations with China and the US and the Role of ASEAN*. *1*, 87–95.

Tu`ân Hưng. (2014). Bi hài chiêu trò của mấ'y 'nhà dân chủ'! Nhân Dân. Retrieved September 16, 2015, from http://www.nhandan.org.vn/chinhtri/binh-luan-phe-phan/item/24344202-bi-hai-chieu-tro-cua-may-nha-dan-chu.html

Tung, N. (2010). Vietnam's Security Challenges: Hanoi's New Approach to National Security and Implications to Defense and Foreign Policies. *NIDS Joint Research Series*, *5*, 107–122. Retrieved from http://www.nids.go.jp/english/publication/joint_research/series5/pdf/5-8.pdf

Ullrich, J., & Cohrs, J. C. (2007). Terrorism salience increases system justification: Experimental evidence. Social Justice Research, 20(2), 117–139. https://doi.org/10.1007/s11211-007-0035-y

Ulum, M. (2017). Cyber Culture and Cyber Security Policy of Indonesia: Combining Cyber Security Civic Discourse, Tenets and Cop enhagen's Securitization Theory Analysis. The 1st International Conference on Social Sciences, (November), 1–2.

Ünver, A., & Kurnaz, A. (2022). Securitization of Disinformation in NATO's Lexicon: A Computational Text Analysis. All Azimuth, 11(2), 211–231. https://doi.org/10.20991/allazimuth.1110500

Valeriano, B., & Maness, R. C. (2015). *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.

Van Dijk, T. A. (2008). *Power and discourse*. London: Palgrave Macmillan.

Van Dijk, T., 1998. Ideology: An Interdisciplinary Approach. Sage, London.

van den Bos, K. (2009). The social psychology of uncertainty management and system justification. In J. T. Jost, A. C. Kay, & H. Thorisdottir (Eds.), *Social and psychological bases of ideology and system justification* (Chapter 8). Oxford Academic. https://doi.org/10.1093/acprof:oso/9780195320916.003.008

van der Toorn, J., Tyler, T. R., & Jost, J. T. (2011). More than fair: Outcome dependence, system justification, and the perceived legitimacy of authority figures. *Journal of Experimental Social Psychology, 47*(1), 127–138. https://doi.org/10.1016/j.jesp.2010.09.003

van der Toorn, J., Feinberg, M., Jost, J. T., Kay, A. C., Tyler, T. R., Willer, R., & Wilmuth, C. (2015). A sense of powerlessness fosters system justification: Implications for the legitimation of authority, hierarchy, and government. *Political Psychology, 36*(1), 93–110. https://doi.org/10.1111/pops.1218

van der Toorn, J., Tyler, T. R., & Jost, J. T. (2011). More than fair: Outcome dependence, system justification, and the perceived legitimacy of authority figures. *Journal of Experimental Social Psychology*, *47*(1), 127–138. https://doi.org/10.1016/j.jesp.2010.09.003

Vasishta, S., & Kapoor, P. (2024). Comparative Trajectories Of Cybersecurity Legislation In Mainland Southeast Asia And China. *Migration Letters*, *21*(S3 (2024)), 1644–1662.

Vargas-Salfate, S., Paez, D., Liu, J. H., Pratto, F., & Gil de Zúñiga, H. (2018). A Comparison of Social Dominance Theory and System Justification: The Role of Social Status in 19 Nations. *Personality and Social Psychology Bulletin, 44*(7), 1060–1076. https://doi.org/10.1177/0146167218757455

Vegh, S. (2002). Hacktivists or cyberterrorists? The changing media discourse on hacking. First Monday, 7(10), n.p.

Vietnam Plus. (2018). Bảo vệ an ninh mạng nhưng không ảnh hưởng đến quyền công dân. Retrieved from https://www.vietnamplus.vn/bao-ve-an-ninh-mang-nhung-khong-anh-huong-den-quyen-cong-dan/495676.vnp (accessed December 10, 2022).

Vietnam Plus. (2018). Chủ tịch nước trả lời cử tri về Luật Đặc khu, Luật An ninh mạng. Retrieved from https://www.vietnamplus.vn/chu-tich-nuoc-tra-loi-cu-tri-ve-luat-dac-khu-luat-an-ninh-mang/508983.vnp (accessed December 10, 2022).

Viet Nam News. (2018). VN cyber security law does not hamper int'l treaties. Retrieved from https://vietnamnews.vn/society/449967/vn-cyber-security-law-does-not-hamper-int-l-treaties.html (accessed December 10, 2022).

Viet, L. T. (2021). Vietnam focuses on cybersecurity and data protection. Retrieved from https://www.russinvecchi.com.vn/publication/vietnam-focuses-on-cybersecurity-and-data-protection/

von Soest, C. & Grauvogel, J. (2017). Identity, procedures and performance: how authoritarian regimes legitimize their rule. *Contemporary Politics, 23*(3). 287-305

Vu, A. N., & Le, B. Q. (2023). The politics of civil society narratives in contestation between liberalism and nationalism in authoritarian Vietnam. *Contemporary Politics*, *29*(2), 182–206. https://doi.org/10.1080/13569775.2022.2102320

Vu, M. T., & Ha, N. D. (2021). Cybersecurity in Vietnam: Legal Framework and Challenges. *Vietnam Law & Legal Forum*.

Vu, N. A. (2017). Grassroots Environmental Activism in an Authoritarian Context: The Trees Movement in Vietnam. *Voluntas*, *28*(3), 1180–1208. https://doi.org/10.1007/s11266-017-9829-1

Vu, P. L. (2019). *Cybersecurity legal frameworks in Vietnam and Japan: A comparative analysis*. Vietnam Japan University.

Wagner, B., Kettemann, M. C., & Vieth, K. (Eds.). (2019). *Research handbook on human rights and digital technology* (Vol. 21). Edward Elgar Publishing Limited. http://journal.um-surabaya.ac.id/index.php/JKM/article/view/2203

Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction(s) and the

production of knowledge about cybercrime. *Information, Communication & Society, 11*, 861-884.

Wang, Z. (2008). National humiliation, history education, and the politics of historical memory: Patriotic Education Campaign in China. *International Studies Quarterly, 52*(4), 783–806. https://doi.org/10.1111/j.1468-2478.2008.00526.x

Wang, X., & Kobayashi, T. (2021). Nationalism and political system justification in China: differential effects of traditional and new media. *Chinese Journal of Communication, 14*(2), 139–156. https://doi.org/10.1080/17544750.2020.1807372

Wæver, O. (1995). Securitization and desecuritization. In R. Lipschutz (Ed.), *On Security* (pp. 46-86). New York: Columbia University Press.

Weldes, J., & Saco, D. (1996). Making State Action Possible: The U.S. and the Discursive Construction of "the Cuban Problem," 1960–1994. *Millennium: Journal of International Studies, 25*(2), 361-395.

Whyte, MK., & Han, C. (2008). Popular attitudes toward distributive injustice: Beijing and Warsaw compared. *Journal of Chinese Political Science, 13*, 29–51.

Wilkinson, C. (2007). The Copenhagen School on tour in Kyrgyzstan: Is securitization theory useable outside Europe? *Security Dialogue, 38(*1), 5–25. https://doi.org/10.1177/0967010607075964

Winseck, D. (2008). Information operations blowback communication, propaganda and surveillance in the global war on terrorism. *International Communication Gazette, 70*, 419-434.

Woollacott, E. (2018). A monopoly on power? Vietnam accused of prioritizing censorship over security. The Daily Swig. Retrieved from https://portswigger.net/daily-swig/a-monopoly-on-power-vietnam-accused-of-prioritizing-censorship-over-security (accessed December 10, 2022).

Wroblewski, J. (1981). Kelsen, The Is-Ought Dichotomy and Naturalistic Fallacy. *Revue Internationale de Philosophie, 35*(138), 508–517.

Yang, S. L., Xu, B. X., Yu, F., & Guo, Y. Y. (2019). Revisiting the status-legitimacy hypothesis: Concepts, boundary conditions, and psychological mechanisms. *Journal of Pacific Rim Psychology, 13*. https://doi.org/10.1017/prp.2019.15

Yang, S. L., Xu, B. X., Yu, F., & Guo, Y. Y. (2019). Revisiting the status-legitimacy hypothesis: Concepts, boundary conditions, and psychological mechanisms. *Journal of Pacific Rim Psychology, 13*. https://doi.org/10.1017/prp.2019.15

Yến-Khanh, N., Phelan, S., & Gray, E. (2022). Neoliberalism and authoritarian media cultures: a Vietnamese perspective. *Media, Culture & Society*, *44*(2), 230-246. https://doi.org/10.1177/01634437211060200

Yeung, A. W. Y., Kay, A. C., & Peach, J. M. (2014). Anti-feminist backlash: The role of system justification in the rejection of feminism. *Group Processes and Intergroup Relations, 17*, 474– 484. https://doi.org/10.1177/1368430213514121

Zhang, Y., Akhtar, N., Farooq, Q., Yuan, Y., & Khan, I. U. (2022). Comparative Study of Chinese and American Media Reports on the COVID-19 and Expressions of Social Responsibility: A Critical Discourse Analysis. *Journal of Psycholinguistic Research*, *51*(3), 455–472. https://doi.org/10.1007/s10936-021-09809-9

Žažar, K. (2022). Fighting the virus, "hunting the witches" – moralizing in public discourses during the coronavirus pandemic in Croatia. *Kybernetes*, *51*(5), 1833–1848. https://doi.org/10.1108/K-11-2020-0819

Zeng, J. (2021). Securitization of Artificial Intelligence in China. Chinese Journal of International Politics, 14(3), 417–445. https://doi.org/10.1093/cjip/poab005

조원선. (2017). Cyber Security Discourses and Securitization Theory: On the Analysis of Korean Cyber Security Issues. *국방정책연구, 116*(December), 145–177. https://doi.org/10.22883/jdps.2017.33.2.006

CURRICULUM VITAE

Academic qualification of the thesis author, Ms. NGUYEN Quang Minh Nguyet:

- Received the degree of Bachelor of Social Science from Hue University of Science, July 2010.
- Received the degree of Master of Arts from Hong Kong Baptist University, November 2017.

November 2024