ISSN 2985-0541 (Print) / ISSN 2539-5513 (Online)

JOURNAL OF CONTEMPORARY SOCIAL SCIENCES AND HUMANITIES

Available online at https://jcsh.rsu.ac.th

Assessing Impacts on Digital Rights and Freedom among Youths under Myanmar's Cybersecurity Law 2025: A Case Study of Youths in Mon State

Minn Myoh Minn Oo, and Jiraroj Mamadkul*

School of Diplomacy and International Studies, Rangsit University, Pathum Thani 12000, Thailand

*Corresponding author; E-mail: jiraroj.m@rsu.ac.th

Received 27 June 2025/ Revised 27 November 2025/ Accepted 3 December 2025/ Publish Online 28 January 2026

Abstract

Nowadays, digital rights and freedom have become as crucial as offline rights across the world as states start restricting these rights using cybersecurity-related laws, disproportionately affecting the digitally most active group 'youths'. In Myanmar, the post-2021-military coup saw the SAC's increasing restrictions on digital rights and the recent 2025 Cybersecurity Law further tightens these restrictions. Being the majority users of digital spaces, youths are most vulnerable to the law's digital constraints on freedom of expression, speech, and information in Myanmar. This study examines the impacts and challenges experienced by youths regarding their digital rights and freedom under the cybersecurity law, through a case study of youths in Mon State. Through a qualitative research approach and a theoretical framework of digital authoritarianism, this study analyzes semi-structured interviews and performs thematic analysis to assess patterns and trends. Findings indicate that youths' digital rights and freedom in Mon State are affected by four significant impacts such as fear of arrest, declining digital engagement, restricted access to information and opportunities, and psychological stress under the cybersecurity law. Additionally, they face four crucial challenges such as VPN criminalization, the law's vaguely worded provisions, digital surveillance and privacy invasion, and inconsistencies in law enforcement. These findings suggest that Myanmar's cybersecurity law is, instead of a legal protector against cybercrimes, a systematic tool of digital repression and authoritarianism, restraining youths' digital freedom.

Keywords**:** *cybersecurity law; digital authoritarianism; Mon State; surveillance; youths*

1. Introduction

In today's digital world, digital rights are crucial for people in their daily communication, educational learning and digital engagement. For youths, particularly in developing and conflict-affected countries, digital spaces are not just social media platforms but also channels for civic participation, mobilization and educational opportunities. The UN Human Rights Council (2016) stated that people must have their human rights protected online the same as offline, meaning that digital rights are fundamental human rights. Moreover, according to Article 19(2) of the International Covenant on Civil and Political Rights (1966), the right to freedom of expression applies to any choice of media platforms for anyone, indicating that free speech and expression are basic rights for everyone on all digital spaces.

Even so, digital rights are not entirely protected across the world. Globally, Kleiner (2025) argued that some countries, especially democratic, use cybersecurity-related laws to prevent citizens from cybercrimes such as digital frauds, identity thefts, and cyberterrorism. However, other countries, particularly with authoritarian motives, take advantage of these laws to monitor and surveil internet use, suppress public dissent, and invade users' privacy, affecting civic digital rights. Since 79% of world internet users are young people aged 15-24 as of 2024 (Kemp, 2025), youths are in the most vulnerable position for these digital rights violations, according to the United Nations (2024).

In Myanmar, 74.7% of internet users are youths aged 18-35 (Kemp, 2024) as of 2024, suggesting that youths in Myanmar are also most susceptible to state digital rights restrictions, like global youths, according to Freedom House (2024). In the pre-coup period, digital rights in Myanmar were relatively more open than in the post-coup. Therefore, Freedom House (2024) reported that the post-coup saw a rapid decline in digital rights and freedom due to state internet shutdowns, censorship, surveillance and criminalization of online dissent. In

addition, Myanmar Internet Project (2025) also stated that because of these digital restrictions, youth activists faced arrest, detention, and violence for their digital activism. Most importantly, the SAC enacted the cybersecurity law on 1 January, 2025, (Lincoln Legal Services (Myanmar) Limited, 2025) and today the law constrains citizens' digital rights and freedoms under digital surveillance and censorship without judicial oversight. Critics such as Human Rights Myanmar (2025) and Myanmar Internet Project (2025) argued that, as primary users of the internet in Myanmar, youths significantly deal with the law's digital restrictions, including criminalization of VPN use, social media blockage, and internet shutdowns.

Despite these digital rights violations, the examination of how the law affects youths' digital rights and freedom under the military government particularly in peripheral regions such as Mon State-remains a significant gap. Culturally diverse and politically marginalized ethnic states like Mon State are often overlooked in existing studies on cybersecurity law and its effects on youths in these states, unlike mainstream regions like Yangon. In fact, Mon State is a particularly fertile ground for this inquiry because of its ethnic diversity, history of political marginalization, and post-coup increase in digital activism among youths within the state (Minority Rights Group, 2017; Athan Myanmar, 2024). These factors make Mon State an ideal case study for assessing the impacts on digital rights and freedoms among youths under the cybersecurity law. Moreover, despite the absence of the latest disaggregated data on the specific percentage of youth internet users in Mon State due to post-coup data suppression, youths still represent a meaningful proportion of the state's and country's youth internet users. By focusing on the case study of Mon State, this study allows for a localized analysis of how the law affects marginalized and digitally active youths in Mon State, offering insights not only for general understanding of other regional disparities but also informing national debates about the law's impacts on digital spaces for youths.

This research is highly significant because it examines the impacts on digital rights and freedoms of youths in Myanmar who are the majority internet users in the country through the case study of youths in Mon State who have been most active in digital activism since the military coup in 2021. The most significant effects on youths in Mon State include 1) fear of arrest and self-censorship, 2) restricted access to information and opportunities, and 3) psychological stress under the law's impacts. These effects limit their ability to use digital spaces to share information, document human rights abuses, and organize protests. Given the law's recent adoption, few studies have focused on exploring specific effects of this cybersecurity law on these youths' digital rights, showing a timely and essential gap in the knowledge. Therefore, this study fills this gap by examining the impacts of the law on digital rights of Myanmar youths and challenges perceived, through a case study of youths in Mon State.

1.1 Definitions of Key Terms

In this research, youths are defined as individuals aged between 21 and 30 who can adequately inform the researcher about their perspectives regarding the impacts of cybersecurity law on digital rights and freedoms.

Moreover, in this study, digital rights are defined as basic human rights such as freedom of speech, expression, and privacy, and access to information and free internet, and these rights must be protected online in the same way as offline.

1.2 Impacts of State Restrictions on Youths' Digital Rights and Freedom in Myanmar

There are three major impacts of state restrictions on digital rights and freedoms among youths in Myanmar, such as restrictions on free expression, limited access to information and opportunities, and weakened digital civic engagement.

1.2.1 Restrictions on Youths' Freedom of Expression

To begin with, freedom of expression has long faced restrictions in Myanmar but the level of suppression was relatively lower in the pre-coup, compared to that in the post-coup. Before the coup, there were several democratic reforms in 2011-2020, resulting in social media platforms, specifically Facebook, becoming one primary space for youths to express their political perspectives and to initiate digital activism (Thein, 2024). However, Thant (2021) argued that state repressive laws such as the Telecommunications Law and the Electronic Transactions Law restricted free digital speech both online and offline, and permitted state

institutions to arrest journalists and youth activists for their opinions that were critical of either the government or the military. Even so, Thant (2021) asserted that in the pre-coup period, youths and activists could still engage in digital dialogues and discussions regarding their political views under relative freedom, using Virtual Private Networks (VPNs). Following the 2021 military coup, the SAC intensified digital restrictions on free speech, imposing internet shutdowns, website blockage and VPN bans. Chew & Jap (2023) posited that state laws enabled the government to constrain digital rights under censorship and surveillance. Because of these restrictions, youths self-censor online, fearing surveillance, arrest, or legal retaliation for involvement in anti-authoritarian expression or activism.

1.2.2 Limited Access to Information and Opportunities for Youths

Another impact is limited access to information and opportunities for youths. In the pre-coup period of 2011-2020, since Myanmar was transitioning to democracy, youths gained increased access to the internet, allowing them more access to information and opportunities. Khine (2023) stated that Myanmar youths could more freely seek professional and educational opportunities online and participate in digital activism on a freer internet before the coup. Also, Thang (2022) contended that Myanmar became one of the most repressive countries in digital rights of Southeast Asia, following the coup. He emphasized that the SAC did not just limit access to electricity but also blocked several websites, resulting in fewer opportunities for youths to access their learning opportunities and information. Even worse, as Proserpio (2024) discussed, these state actions affected more on youths' access to information and opportunities, especially those who were involved in the Civil Disobedience Movement (CDM) as the internet and information access became more restricted to these youths under state digital surveillance.

1.2.3 Weakened Youth's Digital Engagement

Weakened civic engagement was another major impact faced by Myanmar youths regarding digital rights and freedoms. In the years before the coup, youths actively participated in civic engagement through several platforms, particularly in digital spaces. King (2022) defended the idea that youths could participate in student unions, civic protests and political campaigns amidst the country's democratic transition (2011-2020), and that digital spaces acted as primary mediums for them to mobilize digital activism and to initiate policy discussions. Even so, Chew & Jap (2023) criticized that in the pre-coup years, youth-led civic actions still faced several limitations such as repressive state laws and digital restrictions, especially in rural ethnic regions like Karen and Chin states. Moreover, after the coup, these restrictions resulted in a drastic decline in civic engagement by youths due to the military's active crackdowns, digital surveillance and criminalization of political activism on digital platforms. Htwe (2024) asserted that youth-led civic activism was severely cracked down on digital platforms by the SAC, leading to the dismantling of digital venues for youth engagement. He also pointed out that despite these SAC challenges, youths still managed to collaborate in civic-engagement activities such as strike committees and social media campaigns for their political purposes. Consequently, youth civic engagement weakened, affecting their digital freedoms.

1.3 Challenges of Myanmar Youths in Accessing Digital Rights and Freedoms

There are three major challenges that Myanmar youths face in accessing digital rights and freedom in the country such as legal obstacles, restricted internet infrastructure, and state surveillance.

1.3.1 Legal Barriers

The first challenge is legal barriers, which can be further divided into three categories. The first legal struggle is the 2013 Telecommunications Law, specifically Section 66(d) – 'defaming, disturbing, causing undue influence or threatening any person'. This vague term is often condemned by critics because it has been constantly weaponized by the state for the criminalization of public defamation against state actions. Thus, Thein et al. (2017) indicated that citizens' digital rights are significantly undermined under this law because the state often manipulates it to crack down on dissenting views and prosecute both citizens and activists for any critical opinions online and offline.

The second legal barrier is the 2004 Electronic Transactions Law and its 2021 amendment, introducing severe penalties for spreading 'false news'. It has been consistently used by the government over the years for

the suppression of online dissent and for prosecution of journalists and activists, despite its responsibility to regulate electronic communications and digital commerce. That is why, Ochwat (2020) argued that youths' digital rights were limited under this law by silencing their voices or anti-government contents on digital spaces, and that the state takes such free speech as wrongful use of electronic communications under the law's broad worded statute.

The third legal challenge is the 2017 Law Protecting the Privacy and Security of Citizens, as it has been exploited to invade citizens' digital privacy in the name of national security by the state instead of protecting their privacy from external parties' privacy violations. Hence, Athan Myanmar (2018) asserted that digital users' privacy and online history were surveilled and censored by the government without legal oversight, constraining digital freedom. For instance, a 25-year-old youth activist, known as Aung Ko Ko Lwin, was prosecuted under the law for his viral video clip criticizing the Chief Minister of Mon State in 2018, and sentenced to one year's imprisonment.

1.3.2 Restricted Internet Connectivity and Infrastructure

Apart from legal challenges, another key obstacle to youths' access to digital rights is restricted internet connectivity and infrastructure in Myanmar, which are affected by internet shutdowns, power outages and high costs for internet services. Padmanabhan et al. (2021) identified this issue in the post-coup because internet access was restricted by the SAC, limiting broadband coverage, cellular data and telecommunications calls in both urban and rural regions, which further affected information access and online opportunities for citizens, especially youths. Contributing to this, Thida et al. (2023) also flagged the a similar problem in that electricity shortages, internet shutdowns and higher prices for internet and Wi-Fi services were frequent, widening existing digital divide and creating a disproportionate hardship for students and youths from rural areas. Plus, Freedom House (2023a) reported that digital rights in Myanmar were substantially affected by poor internet infrastructure, causing unstable internet connectivity and regular shutdowns. In fact, these digital constraints have not only suppressed digital rights but also contributed to the rise of digital authoritarianism in Myanmar.

1.3.3 State Surveillance and Censorship

One last but most controversial challenge is state surveillance and censorship, as it not only invades users' digital privacy and activities but also bans the use of VPNs and encrypted communications. Here, Padmanabhan et al. (2021) agreed on this point that citizens faced more digital blockage such as certain domain name systems (DNS) and internet protocol (IP) in the post-coup compared to pre-coup, violating their rights to free internet, information and speech. Similarly, Guntrum (2024) denounced these state surveillance activities such that surveillance not only restricted information access but also contributed to arbitrary arrests of youths and activists for their anti-military contents on digital spaces.

Moreover, Freedom House (2023a) reported that the post-coup saw a compulsory requirement for subscriber identity module (SIM) registration for all users and the SAC forced all citizens to re-register using their accurate personal information, which allowed state institutions to surveil and track any dissents easily, violating digital rights to privacy and free expression. In addition, Benjamin & Myint (2024) shared their critique on state surveillance such that surveillance and censorship measures intensified after the coup because extensive closed-circuit televisions (CCTV) were deployed nationwide and technologies were intercepted with telecommunication infrastructure to intensively monitor users' live online activities. Collectively, this issue exposed young people more to privacy violations and deterrence from their digital engagement, violating their digital rights and freedom according to Human Rights Myanmar (2025).

In fact, these challenges are not limited to Myanmar as civilians in other Southeast Asian countries encounter legal constraints on their digital freedoms. Freedom House (2023b) and Sombatpoonsiri & Luong (2022) criticized Thailand's Computer Crime Act 2017 that youths and activists faced criminalization of digital dissent critical of the Thai monarchy and state actions, followed by prosecutions, which place a strict control on Thai youths' digital freedoms. Similarly, Sombatpoonsiri & Luong (2022) and Human Rights Watch (2024) denounced Vietnam's 2018 Cybersecurity Law for its legal authority allowing state institutions to access users' data without requiring judicial oversight, undermining youths' digital activism and promoting digital repression. Furthermore, Cambodia's National Internet Gateway has similar trends as Digital Reach (2021) condemned this law for backing the Great Firewall of Cambodia, promoting state-heavy censorship, surveillance, and privacy

invasion into citizens' data, breaching youths' digital rights. Therefore, youths in Southeast Asia, including Myanmar, are seen to be most vulnerable to the state's digital authoritarian governance.

1.4 Myanmar's Cybersecurity Law 2025 and Its Impacts on Digital Rights and Freedom

The military government officially enacted the cybersecurity law on 1st January 2025, with 16 chapters and 88 articles. The law's Article 5, Clause (g) expresses its obligation to safeguard the development of digital economies using cyber resources within the country. Despite this, it faces several criticisms regarding its cybersecurity measures such as social media blockage, internet shutdowns, VPN restrictions, and digital surveillance of citizens, violating their digital rights and freedoms.

The law allows the SAC to gain full access to user data without any restrictions or judicial approval. According to Article 33, service providers of digital platforms with more than 100,000 users must retain users' personal data, and their digital activity histories for up to three years. Furthermore, if any person or organization with legal authority under the law files a written request, service providers must disclose the information, according to Article 34. Therefore, Myanmar Internet Project (2025) argued that these provisions allow the SAC full access to citizens' digital activities without judicial approval, expanding the state's large-scale surveillance of citizens and their anti-military dissents.

Moreover, the SAC has imposed tighter restrictions on service providers to prevent their attempts to disclose domestic dissent to external parties, as in Articles 42 and 43. In practice, the SAC has toughened its surveillance on both providers and users to monitor their activities critical of the military regime. In addition, because of these provisions, Human Rights Myanmar (2025) criticized the military regime's mass surveillance, data privacy violations, and misuse of citizens' personal information arguing that the lack of transparency and accountability measures over state behaviors allows the SAC's total access to personal information without judicial oversight. Similarly, Myanmar Internet Project (2025) supports the argument that citizens' political dissents are now at more risk of targeted harassment, arbitrary arrests and digital profiling, violating their digital rights, freedoms and privacy.

Subsequently, the law has cut the lifeline of VPN usage for those who bypass state digital restrictions for free information and the internet. Article 29 has criminalized the use of VPNs and digital anonymity by citizens, as it states that anyone found using VPNs or any encrypted messaging applications to bypass state restrictions will be fined heavily and subject to imprisonment. According to Articles 33 and 44, anyone who wants to build VPNs or provide VPN services domestically must obtain state permission and retain users' information for state access. Article 70 further indicates that any unpermitted providers will face either 1-6 months of imprisonment and/or a fine of 10-100 lakhs. These VPN constraints substantially dismantle digital rights of internet users who are now subject to intense state monitoring, censorship and surveillance. Consequently, journalists, youth activists and human rights defenders are disproportionately affected under the law because they rely on VPNs and encrypted communications tools such as Signal, Telegram and ProtonMail to mitigate the risks of legal retaliation and state surveillance. Therefore, ASEAN Parliamentarians for Human Rights (2025) condemned the law for not only violating Myanmar citizens' fundamental freedoms but also for undermining constitutional protections of individual digital rights, noting that it is a formalization of the military regime's increasing violence.

Another controversial component of the law is its broad and vague definitions. Article 72 states that anyone who produces, distributes, sends, copies and sells 'information unfit for public consumption' will be penalized with 1-6 years of incarceration and fines of 10-100 lakhs. Here, there is no specific definition of 'information unfit for public consumption' since the terminology differs across contexts, which allows the SAC to manipulate the term. The same vague provisions can be seen in Articles 60, 62, 64, 66, 71 and 86, where police departments are authorized to perform necessary crackdowns on individuals or organizations who provide critical digital security services and safety without government approval and who violate the law. Therefore, Myanmar Internet Project (2025) further criticized that these provisions put citizens and service providers under constant threat and vulnerability to state arbitrary violence under state surveillance and digital governance, largely affecting citizens' digital rights and freedoms. Strangio (2025) also agreed with this issue, arguing that the law's conferring of overbroad powers to the state allows its censorship of any online anti-regime criticisms and enables the arrest of any dissentients.

1.5 Digital Authoritarianism Theory to the Study

This study is grounded in the theoretical framework of digital authoritarianism (DA), which helps explain how governments exploit digital technologies to suppress public dissent, restrict digital freedoms and control online behaviors, affecting citizens' digital rights. DA is highly relevant in understanding Myanmar's evolving digital governance under the military leadership where laws such as the cybersecurity law 2025 are employed not merely for technical regulation but as digital repression tools for state control.

Polyakova and Meserole (2019) define DA as intentional digital repression used by authoritarian regimes to control their citizens using digital technologies, including digital surveillance and restrictions, constraining their digital activism and engagement in the name of national sovereignty. Expanding on this, Yayboke & Brannen (2020) argue that DA occurs when state leaders with authoritarian intentions employ digital law and technologies to enhance state control over citizens' freedoms, constraining civic free expression. Feldstein (2021) broadens the scope of DA such that both authoritarian and non-authoritarian states may practice digital repression tools such as cybersecurity laws, where governments surveil, coerce, and manipulate citizens' and groups' beliefs and activities critical of their actions through information and technology strategies in the name of national security. Similarly, Michaelson & Ruijgrok (2024) define DA in terms of four dimensions: online censorship, internet shutdowns, digital surveillance, and manipulation of online information, which contribute to restrictions on access to information and free speech. These four strategies contribute to the rise of digital authoritarianism by restricting free speech and expression and suppressing access to truthful information, which leads to severe impacts on digital rights.

This theoretical framework is highly applicable to this study, especially in examining the impacts on digital rights and freedoms among youths in Mon State under the Cybersecurity Law 2025 implemented by the military leadership. The law itself reflects several key features of digital authoritarianism, such as internet shutdowns, digital surveillance, manipulation of online information and state censorship without judicial insight, highlighting theoretical alignment between the law and the theory. This theory helps assess these core characteristics of the cybersecurity law given the institutional nature of the military government and its use of digital technologies for maintaining political power. Applying this theory allows the study to critically assess how the authoritarian government of Myanmar uses the cybersecurity law to constrain youths' digital freedoms under legal restrictions, technological measures and state surveillance and censorship, particularly in politically sensitive regions like Mon State. With a focus on youths in Mon State who are the most active digital users of the population and most vulnerable to digital repression under the law, the theory helps assess how the law affects their digital rights and freedoms.

1.6 Gap in the Existing Literature

While the literature discussed in the preceding sections contains contextual discussion of Myanmar's political context and the rise of digital repression, much of existing scholarship covers the period before 2025 cybersecurity law, leaving a critical gap in assessing the law's impacts after its adoption. Moreover, current research on digital authoritarianism of Myanmar covers less on specific, marginalized groups such as youths who serve as the most digitally active group in the country. Most importantly, many analyses emphasize a broader national-level investigation of digital rights violations, creating a crucial gap for examining sub-national ethnic regions like Mon State. Therefore, this research addresses this gap by assessing the cybersecurity law's impacts and challenges on Myanmar youths through a case study of Mon State by providing primary in-depth findings and transferable novel insights to the knowledge.

2. Objectives

The objectives of the study are (1) to assess the impacts on digital rights and freedom among youths in Mon State under Myanmar's Cybersecurity Law 2025, and (2) to examine major challenges experienced by Mon State youths regarding compliance with the law.

3. Materials and Methods

A qualitative research approach was employed in this study to gain a comprehensive understanding of the impacts on and challenges to digital rights and freedoms among youths under the Cybersecurity Law 2025, through a case study of youths in Mon State. The research is framed around two methods – documentary

research through a systematic review and synthesis of key documents such as the Cybersecurity Law 2025 and academic papers, and semi-structured interviews for primary data collection. A case-study research design was chosen because the research examines a contemporary legal-political issue within a real-world context where law, practice, and personal experiences intersect in complex but meaningful ways (Yin, 2009). The study used semi-structured interview methods to gather primary data sources, and interviews were the best option for the research as they provided free and open forums for key informants to express their perspectives and discuss confidential issues relevant to this study (Guest et al., 2017). It also allowed the researcher to delve deeper into intended information through follow-up clarifications with participants (Merriam & Tisdell, 2016).

In this paper, the researcher's positionality and reflexivity are acknowledged in accordance with the guidelines of critical qualitative research. As an informed independent academic with knowledge of the political and digital landscape of Myanmar, this initially shaped the choice of topic – digital rights – because of a shrinking digital, civic space to amplify marginalized voices of youths. Then, this also shaped data interpretation of findings, resulting in a comprehensive analysis of state power dynamics and effects of digital authoritarianism (e.g. mental stress and fear of arrest). While rigorous measures were ensured to frame the study on the fidelity of participant accounts, this served as a critical lens for data analysis as well, promoting transparency about the researcher's interaction with the topic.

3.1 Participants

A total of seven key informants from Mon State who are associated with and impacted by the Cybersecurity Law 2025 were interviewed. The seven-participant sample size was justified based on the principles of data saturation, in which no new themes were identified from additional interviews (Young & Casey, 2018). By the seventh interview, responses displayed strong thematic convergence, demonstrating that additional interviews would bring only diminishing returns rather than new perspectives. This case-study approach and seven-participant sample size provided rich, in-depth contextual findings and participants lived experiences that fulfil the qualitative nature of this research. However, this may limit the generalizability of findings to the entire population of Myanmar youths, given political complexities and ethnic diversity across other states and regions. Still, these findings serve as transferable results to similar contexts where youths experience digital repression under the law.

The participants were divided into three groups encompassing individual youths, government officials and non-governmental organizations within Mon State. The first group was individual youths from Mon State, selected based on three criteria. They were chosen because they are key persons for the study who can adequately inform the researcher of their personal insights. They must have been born and raised within the state, be at least 21 years old, currently living in their own townships, and have at least 3 years of experience in social work related to digital rights to ensure their relevant knowledge for fulfilling research questions. The second group was government officials because they are focal persons, responsible for enforcing the law within the state, providing credible insights on why and how they enforce the law. Based on three criteria, they must be from the Mon State government office and its related departments, responsible for law enforcement, have at least 5 years of work experience, and be currently working on the issues related to cybersecurity law in their positions. The third group was NGOs within Mon State, because they act as watchdogs within the state and are capable of providing the strengths and weaknesses of the government's policies relative to their intended purposes. Based on two criteria, they must be locally operating within the Mon State working for youths and digital governance, and have worked in these areas for at least 5 years within the region.

Given political sensitivity in Myanmar, participants' safety and confidentiality were strictly maintained. Participants were well informed about the research's purpose, risks and voluntary nature, and informed consent was collected before the interviews. They were notified that they had the right to withdraw any collected information from their interviews at any stage without consequences. No video or audio recordings were undertaken during interviews, and participants were informed that written notes by the researcher for writing purposes only. The researcher conducted all interviews from 22nd to 31st of May. Table 1 shows the list of participants in this research. For the study, the researcher used Participants A, B, or C to protect the identities of key informants.

Table 1 List of Participants

No	Name	Gender	Age	Type of participant	Work experience	Organization
1	Participant A	Male	26	Youth	5 years	Mon State
2	Participant B	Female	25	Youth	4 years	Mon State
3	Participant C	LGBT+	24	Youth	3 years	Mon State
4	Participant D	Female	30	NGO Official	6 years	Mon State NGO
5	Participant E	Female	34	NGO Official	11 years	Mon State NGO
6	Participant F	Male	41	Government Official	8 years	Mon State Government
7	Participant G	Female	38	Government Official	6 years	Mon State Government

3.2 Data Analysis

This study employed thematic data analysis to identify patterns and trends in the impacts and challenges faced by Mon State youths in accessing their digital rights and freedom under the cybersecurity law. It allowed the researcher to analyze qualitative data from interviews and literature and identify common themes that recurred. Following a six-stage thematic analysis of Braun & Clarke (2006), data from interview transcripts were manually read and familiarized several times, which led to the generation of initial codes for responses. This was followed by grouping initial codes into broader themes, which subsequently led to the refinement and review of emerging themes. The fifth phase involved the definition and naming of themes for key impacts and core challenges. Finally, each theme was substantiated through illustrations of participant quotes, thereby producing a comprehensive report of key themes.

Findings of thematic analysis revealed four core impacts and challenges experienced by Mon State youths as illustrated in Tables 2 and 3. The tables below demonstrate the frequency of core thematic impacts and challenges observed across all seven interview samples (N=7). However, it should be noted that two government-affiliated participants consistently provided state-aligned, counter-narratives, either minimizing the severity of these themes or denying their existence entirely. Therefore, the counts below (percentages) primarily reflect the consensus among youth and CSO participants.

Table 2 Key Impacts

Impact (Theme)	Number of participants (N=7)	Percentage of sample (%)
Fear of arrest & Self-censorship	5	71.43%
Declined digital engagement	5	71.43%
Restricted access to information	5	71.43%
Psychological stress	5	71.43%

Table 3 Core Challenges

Challenge (Theme)	Number of participants	Percentage of sample (%)
Legal vagueness	5	71.43%
VPN criminalization	5	71.43%
Fear of digital surveillance	5	71.43%
Inconsistent law enforcement	5	71.43%

4. Results

Findings indicate that there are four major impacts on Mon State youths' digital rights and freedoms under the cybersecurity law - fear of arrest and self-censorship, declined digital engagement and restricted speech and expression, restricted access to information and opportunities, and psychological stress. In addition, it is found that there are four most significant challenges experienced by Mon State youths regarding their digital rights and freedoms under the cybersecurity law: vague legal language and fear of misinterpretation, criminalization of VPNs, fear of digital surveillance and invasion of privacy, and inconsistent law enforcement.

4.1 Fear of Arrest and Self-censorship

A common concern raised by youth respondents in Mon State was fear of arrest and self-censorship when using digital platforms after the law was passed. Participant A (Personal Communication, May 22, 2025) said that before the law was enacted, he felt safer because he could still use VPNs to access blocked websites

and social media applications such as Facebook. Now that the use of VPNs is criminalized under the law, he felt frightened and insecure about his digital identity and privacy. Participants B and C contributed to this discussion, stating they started being more careful with their online behaviors, and refrained from writing any posts, comments, reactions, and shares that are critical of state actions or include sensitive information about the military dictatorship, fearing arbitrary arrests.

In addition, youth participant B (Personal Communication, May 23, 2025) stated, "Last week, one of my friends was arrested at night because of his shared Facebook post of soldiers forcibly recruiting youths for conscription in Mawlamyine within the state. Youths are not really safe in digital spaces anymore."

Similarly, CSO participants echoed the same theme of fear and self-censorship among Mon State youths under the law. Participant D (Personal Communication, May 28, 2025) reported that he noticed a significant decrease in online activities of youths in sharing and posting political content after the law's enactment, resulting in their online behaviors becoming more self-censored and restricted. Contributing to this, Participant E (Personal Communication, May 28, 2025) also shared that their fear of legal consequences led to youths' self-censorship, where they used more anonymous accounts to share content about digital activism against the military dictatorship. Both Participants D and E had expressed their concerns about the law's vague provision about 'information that is not suitable for public view'. Both believed that this legal vagueness was one of the main reasons for youths' fear of digital surveillance and self-censorship for digital safety within the state.

In contrast, government participants from Mon State presented different perspectives. Participant F (Personal Communication, May 30, 2025) from the state government explained that the law simply aimed to create a safe cyberspace where cybercrimes and threats are prevented, and where hate speech is prohibited for the public, including youth populations. He emphasized that nowadays most internet users in Mon State are youths who are digitally active in creating online content, and they may unintentionally or intentionally engage in digital activities harming national sovereignty and public order. Moreover, Participant G (Personal Communication, May 31, 2025) echoed this perspective, stating since the military took over power, youth-initiated digital movements not just in Mon State but also nationwide had facilitated civil unrest, influenced by external groups. Therefore, both participants agreed that the law is crucial for handling all these digital activities from youths within the state to maintain national security and peace.

4.2 Declined Digital Engagement, and Restricted Speech and Expression

Closely related to the fear of arrest and self-censorship, one other impact is Mon State youths' declining digital engagement. Youth participants expressed their concerns about how they find it digitally unsafe to speak up and express their opinions associated with either the military government or revolutionary groups within their cities. Participants A and C (Personal Communication, May 22 & 27, 2025) shared that they became less active on social media by limiting their speech and expression toward sensitive issues because they dared not even trust their online friends, fearing that they might be military supporters and took screenshots of their digital content, and reported it to the police. Moreover, Participant B (Personal Communication, May 23, 2025) also added that she dared not post or text sensitive words such as Civil Disobedience Movement (CDM), SAC, and People's Defense Forces (PDF) on Facebook. That was because she noted an event after the law's enactment, saying "My friend from Thaton (a city in Mon State) was arrested for violating Article 72 of the cybersecurity law for sharing PDF-related news. This case is not in the newspapers. So, fearing this, I do not engage in digital movements for my safety."

Supporting this point, CSO Participants D and E (Personal Communication, May 28, 2025) reflected the same issue for Article 72 and other vague provisions. They raised that these articles particularly caused decreased youth participation in digital spaces within Mon State because before the law, youths were the most active group for speaking up against the military dictatorship, but now, after the law, their digital involvement in these activities showed a significant drop within the state. Participant D highlighted that the provision about information not suitable for public view is a major obstacle because youths' freedom of expression and speech was constrained and they did not actively participate anymore. Then, Participant E voiced that the law, rather than protecting against cybercrimes, was frequently used by local authorities to restrict youths' participation in digital activism.

4.3 Restricted Access to Information and Opportunities

Both youth and CSO participants reported the same issue that, in the aftermath of the cybersecurity law, youths in Mon State lost their access to multiple websites and encrypted applications, losing their access to timely news, information, and opportunities. Youth Participant A (Personal Communication, May 22, 2025) stated that when he used Facebook or YouTube without VPN, most of the content on his newsfeed were related to either entertainment or military propaganda. The news about politics and the revolution did not pop up anymore, and when he searched for news-related Facebook pages, they could not be found. Only when he looked them up through the VPN security, he could check the latest news about conflicts and political issues across the country. Moreover, Participant B (Personal Communication, May 23, 2025) also noted that she had to use VPNs all the time for updates about her online school. Sometimes, she could not connect to VPNs despite her paid subscription due to state digital restrictions on internet connectivity within the state.

Therefore, Participant C (Personal Communication, May 27, 2025) voiced a similar issue, stating "This cybersecurity law may aim to protect against cyber threats on paper but in reality, it not only violates our rights to access to information and news, but also poses security challenges to our digital safety."

CSO participant D (Personal Communication, May 28, 2025) further elaborated that the SAC banned multiple IP addresses, social media applications, and websites, especially those related to the revolution through the firewall under the law. This has tightened existing restrictions on Mon State youths' access to information and learning opportunities digitally.

Participant E (Personal Communication, May 28, 2025) also echoed, "The SAC does not seemingly care about any cybersecurity threats but only its self-interests. The cybersecurity law is just one more authoritarian practice of restricting citizens' rights, mainly youths, in order for them not to challenge the military dictatorship."

On the other hand, government Participants F and G (Personal Communication, May 30 & 31, 2025) stressed that the reason for VPN restriction is to control online gambling activities, cyber security concerns, and information that are not suitable for the public to view and that may cause instability within the state, but not to restrict youths' access to information. Both agreed that the law protects their digital rights but does not violate them.

4.4 Psychological Stress

Psychological stress is another impact raised by youth participants from Mon State under the cybersecurity law. Participant A (Personal Communication, May 22, 2025) indicated that he dared not to join any online groups on either Facebook or Telegram which claimed to be anti-military because he felt afraid that those groups were pro-military ones who tracked down any military offenders. This caused him emotional stress from using online platforms. Participant B (Personal Communication, May 23, 2025) also added that the law officially granted the military government authority to invade her digital privacy and that she lost her digital freedom and privacy. Her knowledge that the military can always trace her digital activities anytime threatened her mental safety when going out in the town.

In addition, Participant C (Personal Communication, May 27, 2025) expressed his psychological stress by saying, "Every time I am online, I refrain from expressing my opinions about any sensitive topics so as not to trigger detections on the SAC's surveillance. This has affected my mental safety online." Participants A and C also explained that their psychological stress caused sleep disturbance on some nights, and they were also frequently discouraged from digitally engaging in social activities with other youths, reducing their digital engagement. Additionally, Participant B also highlighted that her emotional exhaustion sometimes led to self-censoring her online contents for her mental safety, leading to limited speech and expression digitally.

4.5 Legal Vague Language and Fear of Misinterpretation

The most significant challenge faced by Mon State youths was the law's overbroad legal provisions. Participant A (Personal Communication, May 22, 2025) stated that he did not understand what is meant by the 'information not suitable for public view' within the law even though it is written in the Burmese language, because it can mean anything. He shared that this imprecise legal language is a weapon of manipulation by the SAC, allowing local authorities in Mon State to manipulate the law to suppress any dissent. Participant B (Personal Communication, May 23, 2025) further explained her concerns that Article 31 has ambiguously

worded legal clauses such as information that incites hatred, disrupts unity or peace and order, and information inciting to violence. This vagueness confused her about what they mean. She voiced out, "Last month, a few university youths were arrested in Mawlamyine (capital city of Mon State) because the police accused them of their Facebook being found guilty of sharing information that encouraged violence or disrupted state stability. This has made me doubt the law's purpose." Similarly, Participant C (Personal Communication, May 27, 2025) commented that this lack of clarity has led to either intentional or unintentional misinterpretation and allowed those tasked with enforcing the law to manipulate the law for state interests. He said that as a Mon State youth activist who has been a frontliner of the revolution, since he still resides within his township, legal ambiguity in this law posed significant security concerns for his safety, including all youths.

Meanwhile, CSO participant D (Personal Communication, May 28, 2025) agreed that like Articles 31 and 72, Article 70 is vague in describing that anyone who establishes a VPN without permission will be punished. But it does not clarify whether personal VPN use is criminal, even though in practice it is. Then, Participant E (Personal Communication, May 28, 2025) noted, "There have been multiple cases of arrests toward youths in Mon State because of their use of VPNs, and the numbers doubled within the state, particularly after the law. These cases have caused tremendous challenges for them to bypass state surveillance."

From the government's perspective, Participants F and G (Personal Communication, May 30 & 31, 2025) shared that the law is transparent, states everything that will be undertaken, and authorities will check users' data only if necessary, and its purpose is simply to maintain peace and stability in Mon State like other states and regions. Participant G added that the Mon State government publicly announced its responsible committee for enforcing the law and that the government does not hide any information from the public, including youths.

4.6 Criminalization of VPN

Both youth and CSO participants flagged the law's criminalization of VPN use as one of the biggest challenges experienced by Mon State youths. Youth participant A (Personal Communication, May 22, 2025) indicated that since the first day of the coup, VPNs safeguarded his digital activism and information sharing with domestic and foreign fellows by bypassing the SAC's surveillance. This protection helped him to circulate important information about the protests, pro-democracy movements and even financial transactions. Participant B (Personal Communication, May 23, 2025) also pointed out that sometimes, when she transferred the money to either her family or the revolutionary campaigners through local mobile banking such as Kanbawza Pay, she had to use VPNs to erase the traces. Moreover, Participant C (Personal Communication, May 27, 2025) noted that forbidding the use of VPNs has posed risks of arrest and security offline because he shared, "I always delete VPN apps when going out. When I travelled to Ye (a city of Mon State), my bus was stopped at the security checkpoint and soldiers checked passengers' phones, and one male youth was arrested for using a VPN on his phone." In addition, Participant B added that most of the VPN service providers stopped their business and a few still continue but the prices have become more expensive, and youths could not afford it anymore.

CSO participants discussed that although the law does not express anything about the ban of personal VPN use, it is criminalized in practice within the township and country, and most affected are youths within the state because they use digital spaces the most. Participant D (Personal Communication, May 28, 2025) spoke up that the VPN ban affects youths' digital freedom and privacy because they have to use digital platforms daily for their study, entertainment and online activism; however, this law has prevented them from using the VPN. Furthermore, Participant E (Personal Communication, May 28, 2025) added that the VPN ban caused loss of online anonymity for youths within Mon State, especially those related to revolutionary work, and consequently, several youth activists were arrested as they were tracked down by the military under no protection of VPN.

Despite this, government Participants F and G (Personal Communication, May 30 & 31, 2025) explained that in the post-coup, online gambling gained most popularity across the state near the Thai-Myanmar border, and that the cybersecurity law's criminalization of VPNs is essential for taking legal actions against these individuals and businesses. They emphasized that the law helped local authorities to solve these rising cybersecurity threats by tracking gambling businesses within the state. They noted that these are primary reasons for restricting the use of VPNs in the state to maintain state law and order.

4.7 Fear of Digital Surveillance and Privacy Invasion

Another challenge identified by youth and CSO participants was the fear of state digital surveillance and privacy invasion of Mon State youths. Participants A and C (Personal Communication, May 22 & 27, 2025) highlighted that whenever they were online, they felt surveilled, monitored and unsafe under the SAC's digital team. Now that the cybersecurity law is official, their feelings intensified to the extent that they got more scared about the law's approval on invading digital privacy through service providers for the SAC without judicial oversight. Because of this fear, they began to self-censor their content or avoid posting entirely and disconnect from platforms where they feared being watched. Participant B (Personal Communication, May 23, 2025) continued the discussion where the fact that any authorized parties can request users' data from service providers constitutes direct surveillance on youths' digital activities. She said that this affected her digital anonymity since the coup, and deterred her free speech and expression in online spaces. She stated, "Now I dare not post anything anymore and even if it was a joke, I am afraid they will misinterpret it, and the next day, they could be at my door." Participant C further discussed that the VPN ban is such a huge threat to his digital safety and privacy, to be free from state digital surveillance.

Contributing to the same challenge, CSO participants D and E (Personal Communication, May 28, 2025) stressed that the law's requirement of 3-year data retention by service providers, and of authorities being allowed to request these users' data history for checking any online dissents has made youths in Mon State disproportionately at risk from state's surveillance. They expressed that these youths are not sure of what is being watched, how their data is used or what could lead to arrest, but all they know is they are being watched and their privacy and digital identities are not safe. Moreover, the condition where VPNs are criminalized exacerbates youths' digital freedom on online spaces.

4.8 Inconsistent Law Enforcement

Inconsistent law enforcement is another challenge that youths in Mon State encounter. Youth Participants A, and B (Personal Communication, May 22 & 23, 2025) and CSO Respondents D and E (Personal Communication, May 28, 2025) reported that the law's vagueness allowed Mon State authorities tasked with law enforcement to apply the law selectively, targeting youths, specifically male youths, while ignoring others for the same actions. They continued that the law explicitly states that if someone violates it, there are consequences such as fines, imprisonment, or both, but in reality, when youths are arrested, they are released if their parents can pay the amount of money asked by the police or soldiers. In many cases, these arrested youths were sent to the state military base to go into the war. The fine was often not the amount detailed in the law but a higher amount of money. Even though these cases have occurred since the conscription law was enacted, now the cybersecurity has doubled the number within the state, especially for violating the VPN ban. Therefore, Participant C (Personal Communication, May 27, 2025) described, "Sometimes, it does not matter how much money parents give them, their children are taken away for military service because they found VPN apps in their phones. Therefore, I often leave my phone at home because of these inconsistencies."

5. Discussion

5.1 Impacts on Digital Rights and Freedom among Mon State Youths under the Cybersecurity Law

This section discusses four central effects of the cybersecurity law on youths' digital rights and freedom in Mon State, as interpreted through the lens of digital authoritarianism.

Firstly, findings highlight that restricted digital speech and expression are one of the key impacts faced by youths from Mon State on digital spaces under the cybersecurity law. This indicates that their online dissent is restrained, limiting their rights to speak and express their opinions freely, particularly in relation to sensitive political matters. This further exposes their fear of arrest if their digital contents is found critical of the military government. Consequently, they feel compelled to self-censor their contents in fear of state coercion under the law. This finding aligns with Yayboke & Brannen (2020) definition of digital authoritarianism where states customize their digital and cybersecurity laws for coercive control over civic rights of free speech and expression. In this context, the SAC manipulates the cybersecurity law for its self-interests by controlling what youths can and cannot do on digital platforms, constraining their digital freedom. Similar patterns were found in Thant (2021) and Article 19's (2017) arguments where the the Telecommunications Law disproportionately affected youths' digital rights and suppressed their critical comments regarding government actions, resulting in

the state's arbitrary arrests over the years. In addition, these findings also mirror criticisms of the Myanmar Internet Project (2025) and Strangio (2025), in that the law's vague legal language makes youths vulnerable to the state's repressive digital governance on their rights to freedom of speech. Despite these concerns, government Participants F and G (Personal Communication, May 30 & 31, 2025) from Mon State offered a contrasting perspective that the cybersecurity law is important for preventing hate speech and unsuitable information for public view, especially from local youth populations as they are most active on digital channels in order to maintain national sovereignty and stability. Overall, these findings contribute to understanding how laws can be manipulated to restrict youths' digital freedom, strengthening digital authoritarian practices.

Besides these, the findings (Personal Communication, May 22, 23 & 28, 2025) also flag shrinking digital participation among youths in Mon State as another major impact. Such responses reflect that youths' digital privacy and safety are threatened by the law's vague provisions, leading to increased self-censorship. Accordingly, they restrict themselves from expressing their critical views on sensitive content on digital media, resulting in shrinking digital spaces for their online dissent. These findings are consistent with Chew & Jap (2023) discussion where youths' online involvement decreased more in the post-coup because of the SAC's increasing crackdowns on digital dissent and activism through state repressive laws. Hence, this supports Polyakova and Meserole (2019) assertion that states with intentional authoritarian motives to control citizens' digital behaviors use digital laws to restrain their digital participation. In this manner, the SAC under its military dictatorship intentionally employs the cybersecurity law to not only restrict youths' digital rights but also prevent them from engaging in any online activism that are critical of its actions. These findings collectively illustrate the implications of digital authoritarianism in Myanmar's digital landscape, diminishing youths' digital engagement.

Furthermore, findings convey that barriers to accessing digital information and opportunities are another consequence that Mon State youths encounter under the law. This implies that certain information and news, websites and social media, especially related to politics, are censored and blocked by the government. As a result, youths encounter limited information on their cyber spaces as Participant A (Personal Communication, May 22, 2025) and Participant E (Personal Communication, May 28, 2025) mentioned that most of the newsfeed on Facebook are entertainment, and political news are not searchable without VPN. Evidently, this has shown that information and opportunities available on digital spaces are controlled, censored and manipulated by the SAC under the law. This finding resonates with Michaelson & Ruijgrok (2024) discussion on digital authoritarianism where manipulation of online information for state interests is one of the four features of digital authoritarianism. In this sense, youths in Myanmar are manipulated in their rights to free information, and the internet is replaced by military propaganda or entertainment news to keep them distracted from military violence. Similar findings were also reported in Proserpio (2024) criticism where youths' access to online information and opportunity was severely restricted under state surveillance and censorship as the SAC tightened digital restrictions on the use of social media and websites within the country since the coup. Despite these claims, government Participants F and G (Personal Communication, May 30 & 31, 2025) reasoned that the purpose of the cybersecurity law does not lie in intending to restrict any information for youths but rather in keeping them safe from cybercrimes. These findings encapsulate the central tension between two groups - 1) youths, CSO participants and scholars and 2) Mon State government officials. Nonetheless, this issue affects youths' digital rights to free internet, information and opportunities on cyber platforms under the law as one contributor to digital authoritarianism.

Lastly, psychological stress is another chief impact reported by Mon State youths in their access to digital rights and freedom under the law. Although it is not a central focus of existing DA frameworks, it is found in the findings as a significant experiential impact. Youth participants A, B and C (Personal Communication, May 22, 23 & 27, 2025) shared that their psychological security is threatened every time they use their social media accounts and fear that their digital activities could be live-monitored, losing their digital privacy under the law. Their understanding that the SAC can legally invade their privacy under the law's Articles 33 and 34 causes ongoing anxiety and emotional strain, leading to self-censorship and digital isolation. This issue is also indirectly supported by Myanmar Internet Project (2025) where it argued that the law allows the SAC full access to digital users' private information, strengthening their online surveillance. Consequently, this has caused mental insecurity and emotional exhaustion in youths.

All the aforementioned impacts are interrelated and collectively bring significant restrictions on Mon State youths' digital rights and freedom under the cybersecurity law. These impacts reveal that the law is not just a legal regulation but a strategic tool of digital authoritarianism by the SAC, restraining digital privacy, freedom and safety of youths in Mon State.

5.2 Challenges Experienced by Mon State Youths Regarding Compliance with the Cybersecurity Law

In addition to the impacts discussed earlier, this section explores four major challenges faced by youths in Mon State regarding their compliance with the cybersecurity law - VPN restriction, vague legal provisions, digital surveillance and privacy invasion, and legal enforcement inconsistencies.

The findings point out that youths in Mon State perceive the criminalization of VPNs as one of the most significant challenges to their digital freedom under the cybersecurity law. The lack of secure protection like VPNs leads to the loss of their ability to maintain digital safety and anonymity. This increases their vulnerability to state digital surveillance, and to violations of their digital free speech, in terms of political discussion. This reflects Feldstein (2021) definition of digital authoritarianism where states manipulate digital laws and infrastructure to suppress and punish online dissent. In this context, the SAC employs the cybersecurity law's VPN ban for its purpose of coercive control on youths' digital rights to free speech and expression. Similarly, ASEAN Parliamentarians for Human Rights (2025) emphasized that these VPN restrictions not only violate youths' fundamental digital freedoms but also affect their digital activism against the military regime. Therefore, these findings show that the VPN blockage restrains not only youths' digital freedom but also their access to free and open internet and information.

Findings also state that ambiguously worded clauses in the law emerged as another key challenge for Mon State youths. This means that these provisions, such as Articles 31 and 72, are viewed as overly broad by youth and CSO participants even when written in Burmese. This lack of legal clarity has caused confusion and fear regarding how digital actions can be criminalized. This is because findings have shown that the SAC manipulates this vagueness for its self-interests by arbitrarily arresting any online and offline dissents. This imprecise language of the law clearly has allowed the SAC to surveil, coerce and/or manipulate youths' digital behaviors. These provisions have been interpreted by critics such as Myanmar Internet Project (2025) and Strangio (2025), enabling that youths as exposing to the SAC's legal distortion through misinterpretation of the terms or intentional application of the principles where they do not apply. Moreover, this issue aligns with Feldstein (2021) discussion of digital authoritarianism where states suppress dissenting beliefs and legitimize their actions under this vagueness in the name of national security. In Myanmar's context, these overbroad vague provisions of the law are weaponized to seek state interests by exploiting the law, digital technologies and information to restrict youths' digital freedom. Even so, Participants F and G (Personal Communication, May 30 & 31, 2025) maintained that the law is precise enough such that enforcement mechanisms and relevant legal charges are displayed transparently, and denied these criticisms of legal vagueness and distortion. Nonetheless, it is observed that the cybersecurity law's vague provisions are indeed such a threat to youths' digital freedom and privacy.

This leads to another key concern for youths - namely digital surveillance and privacy invasion. These two factors are interrelated such that the SAC can check their online data and invade their privacy under the law, and then surveil them digitally if any actions are found violating the law or track them down and arrest them for exercising their digital rights. These conditions make them vulnerable to the SAC's legal exploitation and put them under constant scrutiny, terrorizing their digital activities. This finding resonates with Guntrum (2024) argument that state surveillance not only oppresses youths' digital freedom but also violates their rights to digital privacy and safety. Benjamin & Myint (2024) also contributed that the SAC's interception of digital technologies with internet infrastructure strengthened its digital surveillance and allowed its live-monitoring and privacy invasion into youths' digital profiles. These findings further reflect theoretical definitions of DA in Polyakova and Meserole (2019) and Yayboke & Brannen (2020) work, such that governments take advantage of digital information and technologies to increase their digital surveillance over citizens' digital activities for their authoritarian motives. In this context, the SAC appears to use digital infrastructure under the law to surveil and invade youths' digital privacy in order to suppress any dissent to maintain its power.

Furthermore, the findings reveal one last but crucial challenges for youths in Mon State which is inconsistent law enforcement by the authorities. Youth participants A, and B (Personal Communication, May 22

& 23, 2025) and CSO Respondents D and E (Personal Communication, May 28, 2025) discussed that local soldiers, police and administration do not adhere to the law strictly but instead misuse its legal vagueness to recruit youths for forced military service or blackmail their parents for a huge amount of money and many cases never reached the court. This challenge is a critical concern for youths' online and offline behaviors and sometimes, the law is used for these local authorities' self-interests. Similar findings were reported in the arguments of Thein et al. (2017), Freedom House (2024) and Athan Myanmar (2018) where the 2013 Telecommunications Law, the 2004 Electronic Transactions Law and the 2017 Law Protecting the Privacy and Security of Citizens were legally distorted to suppress anti-military dissents online. Even though this issue does not directly reflect theoretical frameworks of digital authoritarianism, such inconsistencies express broader concerns over the rule of law and enforcement on the ground for youths.

Overall, the cybersecurity law poses significant challenges to youths in Mon State and their access to digital rights and freedom by the VPN ban, legal restrictions, surveillance and privacy violations, and inconsistent enforcement. Framed through the theory of digital authoritarianism, these insights demonstrate how the law functions as a tool of digital repression rather than protection, particularly for youths.

6. Conclusion

To conclude, this study explored the significant impacts and challenges that Myanmar's cybersecurity law 2025 imposes on the digital rights and freedoms of youths in Mon State, a digitally active group that is most vulnerable to digital repression in the aftermath of the 2021 coup. Through a qualitative case-study approach, it discussed how the law is exploited to restrict youths' digital behaviors, activism and freedom. From the theoretical lens of digital authoritarianism, findings indicate that the law is underpinned by characteristics of digital authoritarianism, functioning as a systematic tool of state digital repression.

Findings show that youths in Mon State experience a shrinking digital space, growing fear of surveillance, privacy invasion, arrest, and mental distress under its law enforcement. Rising challenges such as the ban on VPN use, vague legal language, digital surveillance, and non-uniform enforcement additionally restrict their ability to practice their fundamental digital rights and freedoms, such as free speech, expression, open internet, and digital privacy. Despite government rebuttal of national security and stability objectives, findings suggest that the law strategically restricts digital rights and freedoms in ways that disproportionately target digitally and politically active youths.

Based on the findings, to effectively address the impacts and challenges faced by youths in Mon State under the cybersecurity law 2025, it is recommended that the law's ambiguous worded provisions should be reviewed transparently by independent legal experts and organizations for revisions to align with international human rights standards. Moreover, the use and establishment of VPNs in Myanmar should be decriminalized to protect youths' digital safety and privacy. Furthermore, local and international organizations are encouraged to closely monitor unlawful and inconsistent law-enforcement by local authorities through advocacy and awareness campaigns targeted at youths.

Finally, this study recommends that further research should be conducted by expanding to other states and regions in Myanmar to gain comparative insights across ethnic, geographic and socio-political contexts. Broader data to support generalization could be obtained from incorporating quantitative or mixed methods approaches, for deeper comprehension of impacts and challenges faced by youths regarding their digital rights and freedoms under the cybersecurity law.

7. References

Article 19. (2017). *Myanmar: Telecommunications Lawounit 2013*. Retrieved from https://www.article19.org/data/files/medialibrary/38665/Myanmar-analysis--8-March-2017.pdf

ASEAN Parliamentarians for Human Rights. (2025). *Myanmar Junta's cybersecurity law is unconstitutional and must be withdrawn immediately, says Southeast Asian MPs.* Retrieved from https://aseanmp.org/publications/post/myanmar-juntas-cybersecurity-law-is-unconstitutional-and-must-be-withdrawn-immediately-says-southeast-asian-mps/

Athan Myanmar. (2018). *Research report on prosecution of U Aung Ko Ko Lwin under the "law protecting the privacy and security of citizens"*. Retrieved from https://athanmyanmar.org/wp-content/uploads/2025/01/Eng-Law-Protecting-of-Privancy-.pdf

Athan Myanmar. (2024). *Repression of communication and digital rights situation in Myanmar.* Retrieved from https://athanmyanmar.org/wp-content/uploads/2025/01/REPRESSION_OF_COMMUNICATION_AND_DIGITAL_RIGHTS_SITUATION_IN_MYANMAR-1.pdf

Benjamin, G., & Myint, W. P. (2024). Worse than China or Iran? Myanmar's dangerous VPN ban. *Access Now*. Retrieved from https://www.accessnow.org/myanmar-vpn-ban/?

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Chew, I., & Jap, J. (2023). Youth, identity, and the post-coup experience in Myanmar. *United States Institute of Peace*. Retrieved from https://www.usip.org/sites/default/files/2023-03/ds23-001-youth-identity-post-coup-myanmar.pdf

Digital Reach. (2021). *Online people - Watching: Censorship, surveillance, and the national internet gateway in Cambodia*. Retrieved from https://digitalreach.asia/wp-content/uploads/2021/06/Briefing-Paper-Cambodia-FINAL-1.pdf

Feldstein, S. (2021). *The rise of digital repression*. Oxford, UK: Oxford University Press.

Freedom House. (2023a). *Freedom on the net 2023: Myanmar*. Retrieved from https://freedomhouse.org/country/myanmar/freedom-net/2023

Freedom House. (2023b). *Freedom on the net 2023: Thailand*. Retrieved from https://freedomhouse.org/country/thailand/freedom-net/2023

Freedom House. (2024). *Freedom on the net: Myanmar*. Retrieved from https://freedomhouse.org/country/myanmar/freedom-net/2024

Guest, G., Namey, E., Taylor, J., Eley, N., & McKenna, K. (2017). Comparing focus groups and individual interviews: Findings from a randomized study. *International Journal of Social Research Methodology*, *20*(6), 693-708. https://doi.org/10.1080/13645579.2017.1281601

Guntrum, L. G. (2024). Keyboard fighters: The use of ICTs by activists in times of military coup in Myanmar [Conference presentation]. *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, Honolulu HI, USA. https://doi.org/10.1145/3613904.3642279

Htwe, T. M. (2024). Dynamics of struggle and collaboration: Student and youth activism in Myanmar's 2021 Spring Revolution. In A. Freedman & J. T. H. Lee (Eds.), *RESIST! Democracy and Youth Activism in Myanmar, Hong Kong and Singapore* (pp. 43-66). New York: Pace University Press.

Human Rights Myanmar. (2025). *Myanmar's cyber law a serious threat to privacy, speech, and security*. Retrieved from https://humanrightsmyanmar.org/wp-content/uploads/2025/01/HRM-cyber-security-law-analysis.pdf

Human Rights Watch. (2024). *Vietnam: Repeal harmful internet laws*. Retrieved from https://www.hrw.org/news/2024/12/11/vietnam-repeal-harmful-internet-laws

International Covenant on Civil and Political Rights. (1966). Retrieved from. https://chr-observatories.uwazi.io/en/entity/1ydx0r8divf/toc?raw=true&gad_source=1&gad_campaignid=20825787022&gbraid=0AAAAAo5JJmG1gQJnSiYaK71lbRJFptjPa&gclid=Cj0KCQiAvtzLBhCPARIsALwhxdoK7dZ7f6Wdl3zh1lxGXJP6o6hutoNxnf3mTbu7mZGTRZu-CNLpyfoaArBUEALw_wcB

Kemp, S. (2024). *Digital 2024: Myanmar*. Retrieved from https://datareportal.com/reports/digital-2024-myanmar?rq=myanmar

Kemp, S. (2025). *Digital 2025: Global overview report*. Retrieved from https://datareportal.com/reports/digital-2025-global-overview-report

Khine, N. K. (2023). Digital rights in post-coup Myanmar: Enabling factors for digital authoritarianism. *Journal of Human Rights and Peace Studies*, *9*(2), 186 – 216.

King, A. S. (2022). Myanmar's coup d'état and the struggle for federal democracy and inclusive government. *Religions*, *13*(7), Article 594. https://doi.org/10.3390/rel13070594

Kleiner, J. (2025). How political regimes affect national cybersecurity: The polity flux effect. *Democratization*, *32*(5), 1181-1212. https://doi.org/10.1080/13510347.2025.2451951

Lincoln Legal Services (Myanmar) Limited. (2025). *Cybersecurity law.* Retrieved from https://www.lincolnmyanmar.com/wp-content/uploads/2025/01/Cybersecurity-Law.pdf

Merriam, S. B., & Tisdell, E. (2016). *Qualitative research: A guide to design and implementation.* USA, Jossey-Bass.

Michaelson, M., & Ruijgrok, K. (2024). Digital authoritarianism. In A. Wolf (Ed.), *The Oxford Handbook of Authoritarian Politics*. Oxford University Press.

Minority Rights Group. (2017). *Mon in Myanmar*. Retrieved from https://minorityrights.org/communities/mon/

Myanmar Internet Project. (2025). *The new cybersecurity law and strangling of digital sphere in Myanmar*. Retrieved from https://www.myanmarinternet.info/post/the-new-cybersecurity-law-and-strangling-of-digital-sphere-in-myanmar

Ochwat, M. (2020). Myanmar media: Legacy and challenges. *The Age of Human Rights Journal*, *14*, 245-271. https://doi.org/10.17561/tahrj.v14.5516

Padmanabhan, R., Filastò, A., Xynou, M., Raman, R. S., Middleton, K., Zhang, M., ... & Dainotti, A. (2021). A multi-perspective view of Internet censorship in Myanmar [Conference presentation]. *Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet*, New York, US. https://doi.org/10.1145/3473604.3474562

Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. *Democracy and Disorder*, 1-22. Brookings. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

Proserpio, L. (2024). *Resistance through higher education: Myanmar universities' struggle against authoritarianism*. Bristol: Bristol University Press.

Sombatpoonsiri, J., & Luong, D.N.A. (2022). Justifying digital repression via "Fighting Fake News": A study of four Southeast Asian autocracies. In C. S. Kwok, O. K. Beng, D. Singh, F. E. Hutchinson & N. Saat (Eds.), *Trends in Southeast Asia*. Singapore: ISEAS Publishing.

Strangio, S. (2025). *Myanmar military junta enacts repressive new cybersecurity bill*. Retrieved from https://thediplomat.com/2025/01/myanmar-military-junta-enacts-repressive-new-cybersecurity-bill/

Thang, M. (2022). Unrest in Myanmar after the coup of 2021. In G. Gabusi & R. Neironi (Eds.), *Myanmar after the coup: Resistance, resilience and re-intervention* (pp. 40-53). Toronto, Canada: Torino World Affairs Institute.

Thant, S. M. (2021). *In the wake of the coup: How Myanmar youth arose to fight for the nation*. Retrieved from https://www.boell.de/sites/default/files/importedFiles/2023/10/16/Myanmar%2520youth_FINAL.pdf

Thein, S. S. (2024). *Digital authoritarianism: Implications of military's social media repression on the lives of online activism participants post 2021 coup* (Master's thesis), Central European University, Austria. Retrieved from https://www.etd.ceu.edu/2024/sein-thein_sandi.pdf

Thein, S., Maung, T. S., Win, T. M., & Oo, T. T. (2017). *Burma: Letter on section 66(d) of the telecommunications law*. Retrieved from https://www.hrw.org/news/2017/05/10/burma-letter-section-66d-telecommunications-law?

Thida, M., Thwe, K. Z., Ko, T. K., Thuya, H., Naing, H. E. E., & Hlaing, H. O. W. (2025). Digital disparities in Myanmar: A case study for sustainable digitalization. *Asian Politics & Policy*, *17*(1), Article e70002. https://doi.org/10.1111/aspp.70002

UN Human Rights Council. (2016). *The promotion, protection and enjoyment of human rights on the Internet*. Retrieved from https://digitallibrary.un.org/record/845727/files/A_HRC_RES_32_13-EN.pdf

United Nations. (2024). *Child and youth safety online*. Retrieved from https://www.un.org/en/global-issues/child-and-youth-safety-online

Yayboke, E., & Brannen, S. (2020). *Promote and build: A strategic approach to digital authoritarianism*. Retrieved from https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism

Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Thousand Oaks, California: Sage Publications.

Young, D. S., & Casey, E. A. (2018). An examination of the sufficiency of small qualitative samples. *Social Work Research*, *43*(1), 53–58. https://doi.org/10.1093/swr/svy026