International Journal of Communication 18(2024), 1611–1633 1932–8036/20240005

Intersectional Powers of Digital Repression: How Activists are Digitally Watched, Charged, and Stigmatized in Thailand

JANJIRA SOMBATPOONSIRI♦[1]
German Institute for Global and Area Studies, Germany
Chulalongkorn University, Thailand

This article examines how digital repression tactics—surveillance, prosecution against online activists, and influence campaigns—work in tandem to contain dissent. I applied a mechanism-based approach to analyze interactive patterns of digital repression amidst Thailand's 2020–2021 protests. These were multidirectional. First, digital surveillance provided the intelligence necessary for targeting key dissidents with charges for their online activism. Second, data gathered through surveillance sharpened narratives of proregime cyber troops to stigmatize protesters. Third, smear campaigns gave a pretext for lawsuits against protesters painted as a national security threat. I argue that these mechanisms leverage and reinforce the intersection of panoptic, punitive and framing powers underpinning digital repression, with panoptic power constituting the bedrock. This article speaks to broader studies on social movement repression: Digital repression allows states to deter and incapacitate movements while avoiding backlashes caused by overt crackdown.

Keywords: digital repression, digital surveillance, criminalization, online influence campaigns, dissent, Thailand

On November 23, 2021, at least 17 persons in Thailand received an alert from Apple that their phones were targeted by state-sponsored attackers (*Bangkok Post*, 2021a). In mid-2022, advocacy groups iLaw and Citizen Lab discovered 30 Apple devices of prodemocracy activists, human rights NGO members, and academics infected with the notorious spyware Pegasus (iLaw, 2022). Simultaneously, these targets faced lawsuits, partly because of their activism, while being subjected to coordinated smear campaigns in social media. One cannot

Janjira Sombatpoonsiri: janjira.sombatpoonsiri@giga-hamburg.de
Date submitted: 2023-04-05

[1] My heartfelt thanks go to the interviewees whose insights form the core of this article, and the three anonymous reviewers for their comments. Parts of the research were undertaken during my fellowship at ISEAS-Yusof-Ishak Institute. Earlier versions of this article were presented at the European Association for Southeast Asian Studies Conference (EuroSEAS) in June 2022, the webinar hosted by the Thailand Social Science Seminar Series (TS4) in January 2023, and the onsite panel hosted by the Nordic Institute of Asian Studies (NIAS) in March 2023. I would like to thank Yatun Sastramidjaja, Ward Berenschot, Petra Alderman, and Van Tran for their support of my participation in these events.

help but wonder whether the concurrence of these repression tactics is, by design, creating a symbiotic ecosystem of digital repression. The article sheds light on this phenomenon by asking how repertoires of digital repression are interlinked to maximize hindrances of organized dissent and what kind of power the interrelated mechanisms of digital repression project to deepen control over antielite activism. To advance this analysis, I draw empirical evidence from digital repression in the wake of Thailand's 2020–2021 antigovernment protests.

The article is structured as follows. The first section locates my analytical focus on the current landscape of digital repression studies. Second, I detail how a mechanism-based approach guides my analysis of interdependent mechanisms that render digital repression a powerful vehicle of control, and how data were collected and triangulated. The third section discusses the Thai government's policies to suppress digital space since the 2014 military coup and how these policies were central to curtailing antiestablishment protests in 2020–2021. The fourth section delves into three interrelated mechanisms that underpin digital surveillance, the criminalization of digital activists, and online influence campaigns. In conclusion, I analyze the intersection of panoptic, punitive, and framing powers driving the interactive mechanisms of digital repression.

A Digital Repression Ecosystem to Control Digital Opposition

This study builds on burgeoning research on digital repression by state actors but deepens this by introducing interactive tactics of repression in an ecosystem of digital control. Repression involves state actors' use and threatened use of coercive power to increase the cost of and quell "specific activities and/or beliefs perceived to be challenging to government personnel, practices or institutions" (Davenport, 2007, p. 1; Feldstein, 2021, p. 25). Developing from studies on traditional repression (e.g., Davenport, 2007; Earl, 2011; Mahooney-Norris, 2000), digital repression connotes "the use of information and communication technology to surveil, coerce, or manipulate individuals or groups to deter specific activities or beliefs that challenge the state" (Feldstein, 2021, p. 25). Both democracies and autocracies have increasingly regulated online speech and leaned on high technologies, especially artificial intelligence (AI), for governing dissent (e.g., Earl, Maher, & Pan, 2022), but the control and manipulation of digital space are particularly intense in autocracies that seek to endure popular defiance (Frantz, Kendall-Taylor, & Wright, 2020).

Digital repression repertoires work in tandem in an "ecosystem," referred to in this article as a digital environment in which constitutive components—such as technological infrastructure, service providers, and human operators—interact to foster repression. Despite existing research identifying various repressive tactics (e.g., Bradshaw & Howard, 2017; Chin & Liza, 2022; Ruijgrok, 2021; Sombatpoonsiri & An Loung, 2022), I focus on three repertoires of digital repression—digital surveillance, content manipulation, and the prosecution of digital activists—by shedding light on their interplay. These tactics are common in competitive autocracies that are concurrently classified as middle-income countries like Thailand. As such, repressive apparatus sometimes avoids extreme measures, such as Internet shutdowns, that might negatively affect the vibrancy of the digital economy, while increasingly relying on subtler methods of information manipulation (Feldstein, 2021, p. 47). What follows describes the function of each of these three repertoires. Although it seems that each tactic generates a different effect of control, its function complements one another (Megiddo, 2020).

Digital Surveillance and Panoptic Power

Digital surveillance involves the use of technologies, systems, or legal directives that "enable control through identification, tracking, monitoring, or analysis of individual data or system" (Feldstein, 2021, p. 27). Common subtypes include passive and targeted surveillance, with the former identified as the government monitoring, interception, and retention of data that "has been communicated, relayed, or generated over communications networks to a group of recipients by a 'third party'" (Feldstein, 2021, p. 26). Targeted surveillance is intrusion operations that "manipulate software, data, computer systems, or networks to gain unauthorized access to user information and devices" (Feldstein, 2021, p. 28). Achieving this necessitates surveillance devices, such as the Israeli NSO Group-manufactured Pegasus spyware mentioned earlier (see Marczak, Scott-Railton, Rao, Anstis, & Deibert, 2020). Governments would also need laws related to intelligence and national security to expedite the use of spyware on civilians legally.

As part of a modern surveillance system, digital surveillance projects panoptic power and the power to gaze at and influence behaviors (Manokha, 2018). Social media algorithms, interception technologies, and human monitoring of online content gather all-encompassing "behavioral data" of Internet users, including biometric, geolocation, temporal data, purchase records, private relationships, and more. Similar to tech giants (e.g., Zuboff, 2019), many repressive governments have learned or are learning to instrumentalize this set of data to target dissidents for persecution (Feldstein, 2021, pp. 212–244).

Prosecution of Digital Activists and Punitive Power

Governments and relevant agencies may weaponize laws related to computer information, cybersecurity, and online misinformation to charge, detain, and arrest online dissidents. Overlapping with traditional legal repression (Balbus, 1973), this tactic taps into legal and bureaucratic resources to police and penalize online speeches by critical netizens, journalists, or activists, often with multiple lawsuits, some caused by their social media posts. These charges are piled up against them so that sentences for noncriminal activities, such as clicking "like" on a Facebook post, are harsh, while targets are compelled to expend time and resources in several court cases (Frantz et al., 2020).

Criminalizing online dissent reinforces state power to define what constitutes criminality and to decide when to enforce laws or waive enforcement. This is mostly relevant to states ruled "by law," in which laws are instrumentalized to sustain elites' power and suppress their challengers rather than protect citizens. In this context, the arbitrary enforcement of laws without safeguards for those affected by them is rampant. Whereas elite supporters who allegedly commit crimes benefit from a culture of impunity and evade legal repercussions, dissidents often face charges for noncriminal activities, such as criticizing the authorities online.

State-Backed Social Manipulation and Framing Power

Governments, relevant state agencies, and state-aligned civic groups can manipulate public opinion on social media by tactically circulating false, misleading, and distorted information and doctoring images with the increased help of generative AI models. They also mob or troll online users to disturb conversations and flood existing messages with competing or distracting information (Feldstein, 2021, pp. 32–33; Ong &

Cabañes, 2018). Information manipulation campaigns are carried out by humans and bots (Bradshaw & Howard, 2017, p. 3). Although state institutions and proregime groups predominantly orchestrate information manipulation campaigns, private firms, and citizen influencers have increasingly been involved in these campaigns (Bradshaw, Bailey, & Howard, 2021, pp. 8–9).

As much as technological tools are exploited for social manipulation, existing prejudices, ideologies, and social norms provide discursive sources for such a campaign. Governments can rely on hegemonic frames, including nationalism, to label dissidents as public enemies and threats to national security, thereby mobilizing the public legitimization of governments' responses to threats (e.g., Aron, Edwards, & Handi, 2023). Social manipulation is drawn on predominant frames, while reinforcing the hegemonic power of actors utilizing the frames.

Symbiotic Ecosystem and Intersectional Powers

The interaction of these digital repression repertoires to maximize hindrances of organized dissent remains underanalyzed (Earl et al., 2022, p. 15). Early studies included Gohdes (2014), who argued that the Syrian government tends to shut down the Internet when resorting to indiscriminate violence against civilians in the footholds of rebels. However, it opted for digital surveillance and retained the Internet connection necessary for the targeted repression of opposition movements (Gohdes, 2014, p. 3). Further, Deibert and Rohozinski (2010) illustrate the interlocking relationships of various measures to control and manipulate digital space in Russia, from Internet-related legislations and content filtering to online surveillance and state-sponsored information campaigns on social media (pp. 27–28). The combination of these measures aims to restrict access to oppositional content while building "capacities for competing in information space" of the government (Deibert & Rohozinski, 2010, p. 27). These dynamics also played out in Hong Kong, whose government has simultaneously gathered, disrupted, flooded, and policed digital space while relying on proregime supporters to bully dissidents (Megiddo, 2020, p. 402). Similarly, in Guatemala and Colombia, online disinformation and smear campaigns often intersect with the legal repression of indigenous activists (Wilson, 2022, pp. 9, 13, 18).

This article deepens these insights by unpacking ways in which digital repression tactics symbiotically operate: (1) digital surveillance undergirds the prosecution of dissidents engaged in online activism, (2) personal data gained from the surveillance allows proregime cyber troops to refine narratives that effectively stigmatize protesters, and (3) these smear campaigns, in turn, contribute to justifying legal actions against dissidents. Furthermore, I shed light on how these interactive mechanisms leverage and reinforce the interplay of panoptic, punitive, and framing powers conducive to deterring and incapacitating organized dissent.

A Mechanism-Based Approach and Data Collection Strategies

I apply a mechanism-based approach to the Thai case when illustrating the intersection of different digital repression tactics. Two reasons shape this methodological choice. First, the mechanism-based approach, which originates in a sociological critique of linear causal analysis, allows for theorizing dynamic and multidirectional relations of elements or entities in a given social situation (Abbott, 2001). This coincides with

my objective of capturing how different tactics of digital repression interact and induce interdependent effects, rather than gauging how phenomenon A leads to phenomenon B. Second, when I later derive mechanisms of power from the Thai case, this methodological position encourages a midlevel analysis that possesses some extent of explanatory ability. That is, I can suggest broad theoretical implications of what I have observed from the case without generalizing the findings. This leaves room for theoretical modifications based on the application of alternative methodologies or studies in different cases (Boykoff, 2007).

The data and insights cited reflect (1) state policies and practices identified as methods of digital repression and (2) the experiences of participants in the 2020–2021 protests affected by these policies and practices. The sources of information include news and policy whitepaper archives, social media data, existing NGO databases of affected activists, and semistructured interviews with 12 targeted dissidents and relevant policy actors. I took the following steps to collect and analyze the data. First, in tracing policies and state practices to suppress the 2020–2021 protests, I relied on digitally available official documents. I cross-referenced this with digital archives of news outlets in Thailand, including the English-language newspaper *Bangkok Post* and the Thai media *Prachatai*.

Second, I primarily examined activists' experiences with legal persecution and digital surveillance through NGO databases (e.g., Thai Lawyers for Human Rights and iLaw). In analyzing online smears of dissidents, I delved into content that negatively labeled protesters and behaviors of actors. Through methods of digital ethnography, I spent at least one hour three days a week between February and August 2022 observing posts and interactions on social media pages of proregime outlets—such as *The Mettad*, *Khao Sueak*, and *The Truth*—and civic associations (e.g., Thai Move Institute, Thailand Help Center for Cyberbullying Victims [THCVC]).

Third, I deepened the insights gained from these secondary sources by interviewing 12 individuals between February and December 2022. Ten were concomitantly targeted with online smear campaigns, spywares, and lawsuits, and two were members of parliament who deliberated state-backed surveillance and online manipulation. I identified some targets of repression through the NGO databases detailed earlier and leveraged a snowballing effect for subsequent interviews. These targets are considered prominent dissidents, thereby undergoing multifaceted repression on- and offline. As such, it can be assumed that their views shed light on the interaction of digital repression tactics. The two lawmakers who led parliamentary discussions about the government's misuse of information law and spyware attacks were identified based on news reports. I anonymized the interviewees' names for security reasons.

The Thai Case: How Political Conflicts Shape a Digital Repression Ecosystem

The Thai case was chosen because of two scope conditions: high social media connectivity conducive to contentious digital activism and the government's systematic efforts to curtail it. First, Thailand's social media users have grown steadily, from 60% in 2017 to 80% in 2022 of the 70 million population (Statista, 2023). In 2021, YouTube and Facebook were the most popular platforms, with penetration rates per population of 94% and 93%, respectively (Data Reportal, 2021). Meanwhile, e-commerce in the country is rapidly expanding, with most online retailers depending on their social media accounts for sales (Christopher, 2018).

Second, social media constitutes an important site of communication and mass mobilization in the wake of political conflicts between the country's establishment elites and their challengers. The former encompasses the monarchy, the army, and allied businesses, largely dominating ideological, military, and economic spheres of influence. These actors have historically resorted to coups (most recently, one staged in 2014) as well as armed and unarmed suppression of challengers of the status quo. Contemporarily, these challengers include leaders of opposition parties (previously Pheu Thai and currently Move Forward—the successor of the dissolved Future Forward), their supporters and, recently, the younger generation who spearheaded the 2020–2021 demonstrations. Through the digital mobilization of street protests and online criticisms, these oppositional forces could contest elite power, as is evident in the mass protests of 2009, 2010, 2020, and 2021. This popular dissent exploding in on- and offline spaces echoed an unprecedented "macro-level structural change of Thai society" (*The Straits Times*, 2020, para. 9).

In response, the establishment elites have intensified on- and offline repression. The army cracked down harshly during the 2009 and 2010 protests, resulting in more than 100 deaths. The police forcibly dispersed major protests in 2020 and 2021, injuring dozens. However, as armed repression sometimes caused domestic and international backlashes, the elites opted for unarmed suppression, including judicial and digital forms of harassment. Specifically, under military rule from 2014 to 2019, Thailand's ecosystem of digital repression became increasingly sophisticated. The paragraphs below detail the three primary tactics used: criminalization of online activities, digital surveillance, and influence operations on social media. The interplay of these tactics would come into light during the 2020–2021 demonstrations.

Criminalizing Online Activities

Weaponizing laws for curtailing dissent feature prominently in these toolkits because of the country's longstanding practice of legal-bureaucratic repression (Riggs, 1966). The 2007 Computer-Related Crimes Act (CCA)—amended in 2017—embodies the legal "Goliath" for Internet users. Article 14 theoretically criminalizes anyone creating and/or sharing online content deemed "forged" or "false" that may cause public panic or threaten national security (*Royal Gazette*, 2007, 2017). However, in practice, the CCA is discriminately used against critics of the monarchy, while proregime actors and royalists disseminating disinformation online have hardly been charged (see Sombatpoonsiri, 2022a). This pattern is also evident when CCA is sometimes implemented together with Article 112 or *lèse majesté* and other criminal codes, such as Article 116 on sedition and Sections 326 to 333 on defamation (iLaw, 2010). The CCA-related sentences may be considered mild, with one-year imprisonment and a 20,000 Thai Baht fine (around USD 600). However, violating Article 112 and Article 116 is a serious crime, leading to a maximum seven-year jail sentence. In addition, various bureaucratic and security agencies that normally investigate cybercrimes and security threats have been repurposed to buttress the legal suppression of online subversion. These include the Ministry of Digital Economy and Society (MDES), the police's Technology Crime Suppression Division, and the army's cyber units. Not only can authorities lodge complaints against Internet users, but ordinary citizens are also encouraged to file lawsuits against violators under Article 112.

Lawsuits are a powerful political weapon when individual dissidents and opposition politicians are slapped with several charges to increase sentences. This compels them to expend resources and

energy in court cases; after one lawsuit is concluded, another charge is stacked against them. Although the courts at times acquitted the cases, this decision can take many years, thus keeping dissidents preoccupied with tedious judicial procedures. As we shall see, an emerging practice following the 2020–2021 protests is the courts denying accused activists bail while waiting for hearings, resulting in their detention without conviction. When bail is granted, some activists are compelled to sign a document restricting their participation in political activities and wear electronic monitoring devices to ensure compliance (iLaw, 2021).

Surveillance of Digital Space

The Thai authorities have tapped into the existing security infrastructure and relationships with domestic internet service providers (ISP) to invigorate surveillance systems. Numerous cyber units in the army, the police, and, lately, Interior Affairs Ministry staff have been assigned to monitor social media conversations (*Bangkok Post*, 2016; Juodyté, 2017). In addition to manual surveillance, the police and the Anti-Fake News Centre (founded in 2019 under the MDES) have introduced an automated system akin to social media listening tools to mine massive amounts of social media data (*Komchadluek*, 2020). With this technology, the authorities can track individual users across the social media platforms and even to record the posts, comments, likes, tags, and videos of certain targeted individuals (Sambandaraksa, 2016).

In making digital surveillance more targeted, the Thai government and security forces have allegedly relied on domestic ISPs and interception technologies. Articles 26 and 18 of the CCA require local ISPs to retain traffic data and metadata (information that gives insights into the identities of end users and is stored by ISPs) and grant the authorities access to this series of data on request (I. U. AJN, 2020). In some cases, ISP cooperation is because of existing patronage networks between ISPs' CEOs and the authorities (Privacy International, 2017, p. 10). User data given by ISPs led authorities to track the IP addresses of activists and arrest them (e.g., *Prachatai*, 2020).

Moreover, legal frameworks, such as Article 25 of the Special Investigation Act (2004, amended 2008) and the 2019 Cybersecurity Act and National Intelligence Act, empower authorities to spy on citizens (*Royal Gazette*, 2019a, 2019b). Between 2013 and 2021, the police and the military were alleged to have purchased spy systems from the Italian company Hacking Team and the Israeli NSO (Wikileaks, 2013). These technologies can hack, among other things, mobile phones' emails, and text messages (Draper, 2015; Marczak et al., 2020). The latest spyware the Thai security forces were accused of using against dissidents—Pegasus—has superior technological capabilities, which makes it, for instance, install itself on devices without users taking any action, such as clicking on a malevolent link or switching on microphones and cameras at will (Marczak et al., 2020).[2]

[2] Pegasus' producer is the NSO Group, founded by ex-members of an Israeli intelligence unit and reportedly considered by the Israeli government as a central component of its national-security strategy. Analysts speculate that the Thai government's procurement of Pegasus may be related to Israeli geopolitical advancement.

Influence Campaigns on Social Media

Contemporary state-backed influence campaigns on social media can be traced to the 1960s-70s countercommunism by the military's Internal Security Operations Command (ISOC) but became technologically sophisticated. In safeguarding the monarchy and national security (Nilkamhaeng, 2015), the ISOC currently wages information warfare, possibly hosting 19 to 40 cyber units, each comprising more than 1,000 rank-and-file army personnel, including high school students in the Territorial Defence Command.[3] According to the Oxford Internet Institute, Thai IOs possess a "medium cyber troop capacity" with a wide range of tools and strategies for social media manipulation (Bradshaw et al., 2021, p. 18). The IO units reportedly received basic training workshops about social media content creation and a lump sum of 1,500 Thai Baht (around USD 45) per month. The 2020 annual budget for IOs can be up to 3.7 billion Thai Baht (about USD 110 million). Tactically, IOs seek to attack or devalue opposition figures, commend the regime, and provide partisan information. One IO trooper usually runs several social media accounts at times using inauthentic identifications (e.g., a stock or stolen avatar photo as an account image). He or she would monitor the opposition figures' social media feeds, re-share flagged content with new captions to counteract the opposition's original claims, and respond to antiestablishment posts in the authors' comment section (Sombatpoonsiri, 2022b).

In addition to state-organized IOs, proregime online outlets and royalist civic associations participate in influence campaigns by synthesizing their messages with state-curated content. As such, these groups draw on frames analogous to official narratives, including branding opposition figures as "nation haters," "antimonarchists," and "foreign lackeys." However, one key difference is that grassroots cybertroopers sometimes use their social media platforms to plan the filing of lawsuits against activists accused of offending the monarchy (Sombatpoonsiri, 2022b).

Symbiotic Relationships of Digital Repression Repertoires: 2020–2021 Antiestablishment Protests

Antiestablishment protests broke out in 2020 and 2021, largely because of pent-up frustration against the government and the palace, the latter constituting a threat that particularly alarmed the security apparatus. The protests responded to the establishment elites' power consolidation after the 2014 military coup at the expense of large parts of the population subject to a widening income gap, rampant corruption, and eroding rule of law. In particular, the younger generation saw their future drifting away (e.g., Lertchoosakul, 2021). Because of this, youth support for new and politically outspoken parties, such as the Future Forward Party (FFP), surged. The party attracted 6.3 million of a possible 53 million votes, making it the second-biggest opposition party. Anxious that the FFP would threaten the status quo, in February 2020, the Constitutional Court, an elites' ally, disbanded the party for obscure reasons.

[3] The Territorial Defense Command of the Defense Ministry offers a military training course for high school students. Upon completion after three to five years, graduating students are exempted from annual military conscriptions.

Enraged, young people protested, first in March 2020 before the COVID-19-related lockdown, from June to December 2020, and second from April to September 2021. The mid-2020 protests were arguably the largest, most innovative, and most controversial since the 2014 coup. More than 600 protests, with the largest event having almost 100,000 participants, were organized nationwide. Youth movements, led by Free Youth and the United Front of Thammasat and Demonstration (UFTD), relied on social media and other digital tactics for mass mobilization (Sombatpoonsiri & Kri-aksorn, 2021). Most importantly, activists' demands included democratic reforms of the monarchy; many protest speeches and online discussions were seen as contemptuous of the palace (Wongcha-um & Johnson, 2020). As a result, security forces stepped up crackdowns on dissent on- and offline. When mass protests critical of the government's COVID-19 mismanagement recurred in mid-2021, the regime was well prepared and could effectively undermine the protests, which had already faced an internal crisis (C and F, personal communication, July 6 and 27, 2022). The two-year mass uprisings witnessed the growing intersection of the three digital repression methods described previously. The following sections analyze their dyadic relationships in which one tactic facilitates another or actors driving the dual tactics overlap.

The Nexus Between Digital Surveillance and Criminalizing Internet Users

Based on events unfolding during the 2020–2021 protests, it appears that digital surveillance enables authorities to effectively identify activists accused of violating the laws while gaining access to evidence for lawsuits. From late 2020 to February 2023, 233 individuals involved in antiestablishment activism were charged with Article 112, most simultaneously facing CCA-related charges (TLHR, 2023). Two sets of actors engage in the human-based monitoring of online feeds to gather evidence for lawsuits: security forces and grassroots vigilante groups. By working with ISPs, the former could track the IP addresses of activists whose posts are deemed to violate these laws. The authorities also physically followed and took pictures of activists at protest sites while retrieving records from CCTVs installed around Bangkok. According to two activists I interviewed, these materials are sometimes used in courts (J and L, personal communication, August 10 and 17, 2022). One of them was charged with tampering with the 2016 constitutional referendum by tearing his ballot. During a court hearing, he claimed that a staff member from a telecommunication company testified as an expert witness: "This expert specifically told the judge when and how many times I was contacting two other friends who were live-broadcasting my activity … and the geolocations of our calls in line with the timeline of that activity" (L, personal communication, August 17, 2022). This was cross-referenced with evidence from the police, leading the court to convict him.

In the wake of the Pegasus exposé in late 2020 and the resurgence of protests in mid-2021, targets of legal persecution seemed to shift from prominent activists to movement supporters working behind the scenes. This led activists to suspect that the authorities might gain confidential data about these supporters through spyware. The most telling cases are activists allegedly responsible for funding management and public relations, all attacked by Pegasus. The name of Activist J appeared on a bank account that received public donations for a movement's activities. On September 17, 2021, the cyber police raided her residence when she was with two other activist friends. She was the only one facing two serious charges: Article 116 (sedition) and computer crimes (Nation TV, 2021). She believed that the arrest was not only because of her name on the bank account but also because of her status as an administrator of the UFTD Facebook Page.

J was puzzled by the authorities' insight because she had kept this information a secret and never used a personal account to operate the group's official account (J, personal communication, August 10, 2022). H, J's activist friend, was also attacked by Pegasus during this period. He suspected that the authorities were scrambling for information about other administrators of the UFTD Page to slap them with charges (H, personal communication, July 29, 2022).

Two other activists, in charge of the financial support and logistics of the movements and targeted with Pegasus, expressed similar concerns. They were aware that the authorities had kept taps on their online banking information, nervously expecting impending charges based on, for instance, the exploitation of tax evasion allegations. They feared that through Pegasus, the authorities might get insights into the movement's donors and pursue legal action against them (F and I, personal communication, July and August 4, 2022). Whereas some Pegasus targets I interviewed were unsure whether private data unlawfully obtained by the spyware could be used in courts, it seems that at least disclosing "secrets" about the movement helped the officers connect the dots, pointing to where they could get evidence for the lawsuits against these dissidents. At times, activists suspected that the authorities might snoop on confidential information about protest plans to preemptively slap activists with charges, thereby preventing protests from taking place (F and H, personal communication, July 27 and 29, 2022).

In most cases, social media monitoring by tens of thousands of cyber troopers is sufficient for gathering evidence for lawsuits. Leading activist and human rights lawyer Arnon Nampa has been slapped with two Article 112 lawsuits and 15 other charges, some of which pertain to the CCA (TLHR, 2022). On filing complaints, the police and attorney could present detailed evidence based on Arnon's Facebook posts, video clips, and other online records (TLHR, 2022). Similarly, the leading protest organizer, Panusaya Sithijirawattanakul has been repeatedly charged with Articles 112, 116 (sedition), the CCA, among others. The authorities presented the court with elaborate evidence, including specific words in Panusaya's speeches that they deemed *lèse majesté.* Ordinary netizens have also been charged with Article 112. As of February 2023, 119 of 151 lawsuits targeted posts, comments, and visual content on social media (TLHR, 2023), with the accused as young as 14 years old (*Prachatai*, 2022). Of this number, 84 cases were filed by citizens and royalist vigilante groups, such as the THCVC and Monarchy Protection Group (TLHR, 2023).

In precisely targeting people for lawsuits, it seems that these groups would have to monitor social media feeds on Facebook or Twitter that the authorities might flag. The confluence of the two circumstances substantiates this assumption. First, various complaints were filed against those leaving comments under Twitter posts by exiled dissidents, such as Somsak Jiamtirasakul or sharing content originally posted on the opposition groups' Facebook Pages, such as Royalist Market Place (TLHR, 2023). Without round-the-clock surveillance of feeds on these pages, the lawsuits would not have been so curated and crafty. In at least one case, an individual accused another individual of circulating a *lèse majesté* post through the private chat application LINE. Second and relatedly, members of the THCVC admitted to collecting evidence and sharing them in the private chat group. A THCVC activist claimed that its members were trained on how to file an Article 112 complaint and had received a guide on how to do so from the private chat group: "We have our LINE chat room in which information [about *lése majesté* cases] are shared. We discuss who will be responsible for filing what cases and in which provinces. We gather all the evidence" (Phanttapak, 2021, para. 14). Additionally, the group created a Google map that identified the addresses of hundreds of Article

112 offenders (*Prachatai*, 2021; Figure 1) and deliberately filed complaints at a provincial police station far from the accused's residences. This created extrahurdles, such as travel costs and time spent on trips (Phanttapak, 2021).

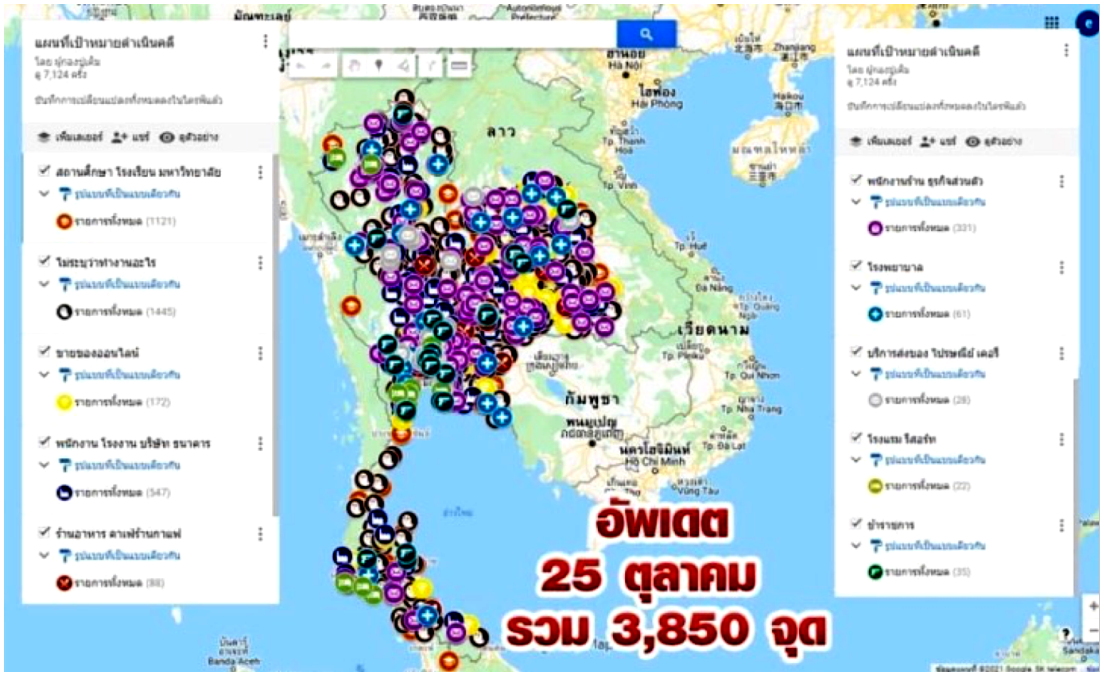

Figure 1. THCVC's map identifying 3,850 addresses of Article 112 violators and locations where offenses occurred (*Phanttapak*, 2021, para. 17).

The Nexus Between Digital Surveillance and Online Influence Campaigns

Digital surveillance and online influence campaigns operate symbiotically because of the crossover between surveillent agents and smear campaigners and the use of spyware that sharpens "frames" against dissidents. Through the crossover between actors, information, and narratives unfavorable to dissidents are shared and amplified. Take, for example, THCVC's Facebook page, which shares posts flagged as offending the monarchy and simultaneously distributes content from proregime outlets, such as *Top News* and "royalist influencers." These sites are known for popularizing frames that vilify critics of the government and the monarchy as "nation haters" (*chang chart* in Thai), foreign lackeys who sell the nation (*khai chart*) in Thai, and morally corrupt people (Sombatpoonsiri, 2022b). In so doing, the THCVC not only surveils dissidents' online behaviors but also reinforces narratives underpinning smear campaigns. For instance, of 400 posts by the THCVC between February 2022 and 2023, several dozens of posts were content re-shared from *Top News*. On July 19, 2021, the THCVC reposted the accusation by Suphanat Aphinyan, a well-known royalist influencer, that the opposition figureheads—Thanathorn Jungrungreongkit and Piyabutr Saengkanokkul—sought to overthrow the monarchy. This allegation has persistently circulated among royalists who interpret these figureheads' critical stances toward the monarchy as a threat to be contained (e.g., *BBC Thai*, 2019).

In contrast, royalist mouthpieces orchestrate smear campaigns by deriving content from surveillent pages like the THCVC or, at least, promoting its legal vigilantism. For example, in the wake of the 2021 protests, *Top News* frequently published reports of the THCVC filing lawsuits against alleged monarchy offenders (e.g., *Top News*, 2021).

Moreover, the reliance on technology for surveillance in Thailand means that dissidents' personal information and organizational secrets can be disclosed and instrumentalized for online influence campaigns. For instance, two academics I interviewed were attacked by Pegasus in 2021. They supported student activists—using their professional positions to bail the accused—or published research critical of the military or the palace. As with other oppositional intellectuals, they have concurrently been slandered by proregime outlets for backing trouble-making students (e.g., *The Truth*, 2022) and spreading "lies" in the guise of historical knowledge that undermines the monarchy (e.g., Thai Move Institute, 2020a). Although there is no evidence that private information leaked through spyware has been used against them, these figures are concerned that this could happen if the crackdown intensifies in the future. According to one academic, "[through Pegasus] the authorities may take a picture of me in private space like the bedroom when I wear whatever I like… This may be doctored and inserted with a caption that negatively frames me" (E, personal communication, July 19, 2022).

In other cases, cyber troops may use leaked information, for instance, about the financing of the movement or intraorganization disputes, to baselessly claim that the leading activists embezzle public donations for the movement or abuse power for their own gains (F and L, personal communication, July 27 and August 17, 2022, respectively). Activist L, which helped safeguard protesters on-site, considered some of the information that cybertroops posted on their pages (e.g., the Twitter account "Jae Juk Klong Sam") to be confidential; he was surprised that it got out. He suspected that this was either because of a potential infiltrator within his organization or spyware (L, personal communication, August 17, 2022). For activist F, who managed movement funding, surveillance-induced influence campaigns can push the narrative that sows internal mistrust. For instance, in March 2021, proregime outlets circulated pictures of her "pampering," leading activists with expensive meals and drinks, causing other activists to question whether the funding was misused and demanding that she be more transparent. F suspected that this framing was linked to the authorities' monitoring of her activities, including fundraising and financial management:

> I was attacked by Pegasus because I was one of the two people responsible for the movement's bank account…when IO [troopers] learned that I primarily arranged food, water and mobile toilets for the protesters, they started attacking me based on this information (F, personal communication, July 27, 2022).

This initial smear was picked up by other movement members. For F, their mistrust is disheartening, while posing a dilemma. Financial transparency would force her to reveal not only expenses but also sources of the movement's funding, which would put undisclosed donors at risk. However, her failure to respond to this demand meant that she could not defend herself from the accusation (F, personal communication, July 27, 2022). This example is among the many instances in which leaked exclusive information was weaponized for online influence campaigns to drive rifts within the movement.

The Nexus Between Online Influence Campaigns and Criminalizing Internet Users Nexus

Lastly, online influence campaigns intersect with the criminalization of online dissidents by stigmatizing them to set the scene for lawsuits. Although it is difficult to trace whether a specific influence campaign directly correlates with a lawsuit against dissidents, we can still associate a frame that stigmatizes activists with building political momentum for legal harassment. The accusation of domestic dissidents as "foreign lackeys" is a standard frame of proregime cybertroops. Prodemocracy movements and opposition parties are often portrayed as collaborators with the West, specifically the United States, at the expense of the country's traditional pillars. During the 2020 and 2021 protests, this frame gained traction among proregime groups, who accused leading activists, public intellectuals, and opposition politicians of taking "Western" money to destabilize the country. The Thai Move Institute and its affiliated outlets posted a diagram of this conspiracy on its Facebook page (Figure 2) by linking the opposition figures who spearheaded the 2020 protests with the U.S.' National Endowment for Democracy (NED) and international organizations such as Amnesty International (AI) Thailand and Human Rights Watch.

Soon after, cyber troops "mobbed" AI's Facebook page for working for foreign interests by supporting young activists to undermine national security, with several posts apparently repeating the same messages.[4] Royalist news sites then started calling for the eviction of AI (e.g., *The Truth*, 2021a). Among other royalist influencers, the former director of the National Intelligence Agency posted on his Facebook that he wanted to see Amnesty Thailand evicted from the country, the message in line with the campaign #AmnestyGetOut (*Manager Online*, 2021). In this light, AI faced a series of legal intimidations by the authorities. For instance, in early 2022, the Ministry of Internal Affairs, with which Amnesty Thailand registers, threatened to investigate its foreign funding and legal status in Thailand (*Thai Post*, 2022). Meanwhile, the authorities pressured AI's East and Southeast Asia office, based in Bangkok, that its registration would be discontinued if AI Thailand "causes trouble."[5]

[4] Amnesty International Thailand kindly shared its documentation of abusive comments under its posts. AI staff observed that some of these comments seemed to copy and paste from one another.

[5] This information comes from AI Thailand's internal document its leadership shared with this author.

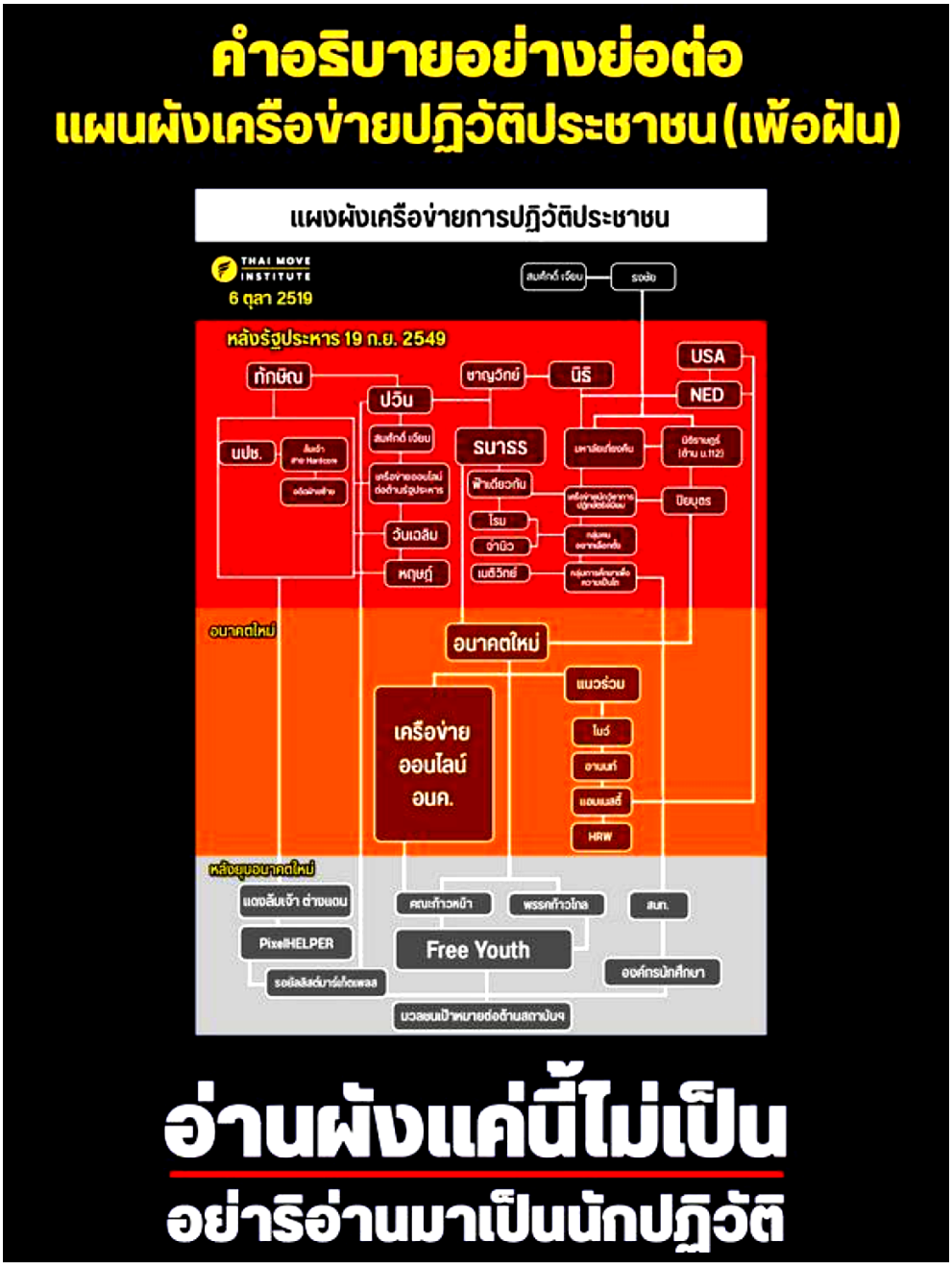

Figure 2. ***"Diagram of People's Revolution" published by the Thai Move Institute depicts networks of "revolution by the opposition movement," with Future Forward Party at the center (in orange tab), youth activist groups below it (in gray tab), and international supporters including NED and U.S. government at the top (in red tab; Thai Move Institute, 2020b).***

Similarly, the frames of "foreign lackey" and "antimonarchy nation haters" create a discursive ground for legal harassment by progovernment forces. In countering the 2020–2021 protesters' demand to reform the monarchy, royalist cyber troops and news outlets propagated the claim that protesters harbored malicious intent against the palace (Thomas, Beattie, & Zhang, 2020). In the Thai context, this allegation is situated in asymmetrical information warfare in which those framed to defame the monarchy can be heavily penalized. Based on my keyword search in the online archive of the royalist mouthpiece *The Truth*, the first mention of protesters violating the monarchy appeared in September 2020. Calls for jailing protesters alleged to challenge the monarchy intensified from October onward. Against this backdrop, the authorities reintroduced Article 112 in November that year after three years of not using it.

In the aftermath of the 2020–2021 protests, social media campaigns denouncing offenders of the monarchy have persisted, in parallel with royalists actively filing charges against online offenders. For instance, Seri Wongmontha, a royalist mouthpiece, posted on his Facebook that many who joined the 2020 protests deserve to be arrested because they "violated the law…[and] tainted the king's reputation…" (*Siamrath*, 2022, para. 1). He considered those accused of violating Article 112 to sell out Thailand to foreign countries to "hate their nation" (*Siamrath*, 2022, para. 1). Furthermore, as royalist influencers accused NGOs, such as iLaw, to conspire with foreign powers against the monarchy (e.g., *The Truth*, 2021b), many iLaw staff were subject to several lawsuits. This included Yingcheep Atchanon, slapped with 11 charges after giving protest speeches in 2021. Other prominent activists, including Panasaya and "Penguin," charged with Article 112 and repeatedly detained, have also been similarly framed as attempting to overthrow the monarchy and being on Western payroll (e.g., *The Truth*, 2021c).

The intersection between online framing and the criminalization of social media users was palpable in the November 2021 ruling of the Constitutional Court. In 2020, a staunch royalist and former advisor to the Thai Ombudsman submitted a petition to the court to decide whether the 2020 protesters' demands violated Article 49 of the Constitution concerning regime change (*Bangkok Post*, 2021b). Despite protesters' claim that their demand was about reforming rather than toppling the monarchy, the court ruled in November 2021 that protesters violated the Constitution's Article 49 for "hidden intentions to overthrow the constitutional monarchy" (*Reuters*, 2021, para. 3). This ruling seems to echo the rhetoric of royalist cyber trolls, who slander activists as antimonarchy day in and out. The ruling, in turn, provides a further basis for the authorities' legal action against other critical activists, academics, and political parties (*Bangkok Post*, 2021b), resulting in a significant rise in *lèse majesté* lawsuits in November 2021 (TLHR, 2023).

Conclusion: Implications of Intersecting Digital Repression on Power Dynamics

In the Thai case, the three forms of digital repression—criminalizing Internet users, digital surveillance, and online influence campaigns—work in tandem to increase the costs of dissent and ultimately foster effective control of it. At the heart of this analysis is the nexus of "costs" and control: What kinds of costs are invoked by the symbiotic ecosystem of digital repression? And what kind of control do such dynamics produce? This article has illuminated how the interdependence between digital surveillance, online influence campaigns, and criminalizing Internet users has allowed Thai authorities to identify key activists and supporters for propagandistic labeling and targeting them with specific charges. Based on these mechanisms, I make the following theoretical observations. First, traditional surveillance enables state

control through ubiquitous "gaze" (Foucault, 1977), prompting intelligence gathering and dissidents' self-censorship (Manokha, 2018). Built on this panoptic power, advanced technologies, particularly AI, render the collection of dissidents' data increasingly fine-grained. This boosts the prediction ability of governments in the face of organized dissent, enabling its curtailment preemptively through arrests and manipulated public opinion unfavorable to activists.

Second, online influence campaigns drawn on hegemonic frames, such as nationalism, security, and moralism, serve to stigmatize dissidents in a broader societal and political context. This framing power can undermine public support of a movement and even justify the authorities' judicial and forcible crackdown on dissidents labeled as threats to national pillars. Framing power underpins this stigmatization, which yields spillover impacts on activism and dissidents' personal lives (Boykoff, 2007, p. 296).

Finally, framing and panoptic powers reaffirm punitive power. Identified for arrests or framed as unpatriotic, dissidents face multiple charges that compel them to expend their time, limited financial resources, and the energy to fight multiple court cases. Further, this tactic dilutes the movement's focus on political advocacy, shifting public attention from its core demand for change to relentless lawsuits. Ultimately, punitive power characterizes legal charges and tedious judicial procedures that lessen a movement's ability for "resource mobilization" (Boykoff, 2007, p. 294).

I argue that panoptic power constitutes the bedrock of these intersectional mechanisms of control. Without extensive and in-depth information on individual activists and their activism, legal charges and information manipulation would not have been targeted. In the age of "big data," which empowers AI- and human-based surveillance, data are key to the effective deterrence of state challengers.

This insight speaks to broader studies on the state repression of social movements that have increasingly moved beyond overt repression through armed violence. Over the past few years, armed crackdowns on mass movements have caused backlashes, especially by further encouraging mass resistance (e.g., Chenoweth & Stephan, 2011; Lichbach, 1987). Coping with these backlashes, various regimes have increasingly relied on unarmed and covert repression to strategically incapacitate movements (e.g., Moss, Michaelsen, & Kennedy, 2022). This article complements this discussion by highlighting how the symbiotic ecosystem of digital repression leverages and deepens panoptic, punitive, and framing powers to hinder effective mobilization. Future research should reinvestigate the mechanisms proposed in this article through comparative cases, explore new forms of digital repression as technologies evolve, and propose ways in which dissidents can counter digital repression.

References

Abbott, A. (2001). *Time matters: On theory and method*. Chicago, IL: Chicago University Press.

Aron, D., Edwards, P., & Handi, L. (2023). Message or messengers? Sources and labeling effects in authoritarian response to protest. *Comparative Political Studies, 56*(12). doi:10.1177/00104140231168361

Balbus, I. (1973). *The dialectics of legal repression*. New York, NY: Russell Sage Foundation.

Bangkok Post. (2016, November 1). Army tightens monitoring of social media. Retrieved from https://www.bangkokpost.com/thailand/general/1124460/army-tightens-monitoring-of-social-media

Bangkok Post. (2021a, November 24). Apple warns Thai activists 'state-sponsored attackers' may have targeted iPhones. Retrieved from https://www.bangkokpost.com/thailand/general/2221003/apple-warns-thai-activists-state-sponsored-attackers-may-have-targeted-iphones

Bangkok Post. (2021b, November 10). Constitutional Court rules activists aimed to overthrow monarchy. Retrieved from https://www.bangkokpost.com/thailand/politics/2213147/constitutional-court-rules-activists-aimed-to-overthrow-monarchy

BBC Thai. (2019, December 22). Future forward: Constitutional court schedules hearing to dissolve Future Forward Party based on the Illuminati complaint. Retrieved from https://www.bbc.com/thai/thailand-50883633

Boykoff, J. (2007). Limiting dissent: The mechanisms of state repression in the USA. *Social Movement Studies, 6*(3), 281–310. doi:10.1080/14742830701666988

Bradshaw, S., Bailey, H., & Howard, P. N. (2021, January 13). *Industrialized disinformation: 2020 global inventory of organized social media manipulation*. Computation Propaganda Research Project, Oxford Internet Institute. Retrieved from https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf

Bradshaw, S., & Howard, P. (2017). *Troops, trolls and troublemakers: A global inventory of organized social media manipulation* (Working Paper No. 12). Retrieved from https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

Chenoweth, E., & Stephan, M. (2011). *Why civil resistance works: The strategic logic of nonviolent conflict*. New York, NY: Columbia University Press.

Chin, J., & Liza, L. (2022). *Surveillance state: Inside China's quest to launch a new era of social control*. New York, NY: St. Martin's Press.

Christopher, M. (2018, August 3). *Social media boom in Thailand leads to a rise in social commerce*. OpengovAsia. Retrieved from https://opengovasia.com/social-media-boom-in-thailand-leads-to-a-rise-in-social-commerce-in-thailand/

Data Reportal. (2021). *Digital 2021: Thailand*. Retrieved from https://datareportal.com/reports/digital-2021-thailand

Davenport, C. (2007). State repression and political order. *Annual Review of Political Science, 10*(1), 1–23. doi:10.1146/annurev.polisci.10.101405.143216

Deibert, R., & Rohozinski, R. (2010). Control and subversion in Russian cyberspace. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zinttrain (Eds.), *Access controlled: The shaping of power, rights, and rule in cyberspace* (pp. 15–34). Cambridge, MA: MIT Press. doi:10.7551/mitpress/8551.001.0001

Draper, J. (2015, July 25). Thailand acquires advanced electronic surveillance police state capability. *Prachatai*. Retrieved from https://prachatai.com/english/node/5345

Earl, J. (2011). Political repression: Iron fists, velvet gloves, and diffuse control. *Annual Review of Sociology, 37*(1), 261–284. doi:10.1146/annurev.soc.012809.102609

Earl, J., Maher, T., & Pan, J. (2022). The digital repression of social movements, protest, and activism: A synthetic review. *Science Advances, 8*(10), 81–98. doi:10.1126/sciadv.abl8198

Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford, UK: Oxford University Press. doi:10.1093/oso/9780190057497.001.0001

Foucault, M. (1977). *Discipline and punish. The birth of the prison*. New York, NY: Vintage Books.

Frantz, E., Kendall-Taylor, A., & Wright, J. (2020). *Digital repression in autocracies* (V-Dem Working Paper). Retrieved from https://www.v-dem.net/media/publications/digital-repression17mar.pdf

Gohdes, A. R. (2014). *Repression in the digital age: Communication technology and the politics of state violence* (PhD dissertation). University of Mannheim, Mannheim, Germany. Retrieved from https://madoc.bib.uni-mannheim.de/37902/

I. U. AJN. (2020, July 1). Internet service providers are helping the Thai government track down dissidents. *New Mandala*. Retrieved from https://www.newmandala.org/internet-providers-are-helping-the-thai-government-track-down-dissidents/

iLaw. (2010, December 8). *Situational report on control and censorship of online media, through the use of laws and the imposition of Thai state policies*. Heinrich Boll Stiftung Southeast Asia. Retrieved from https://th.boell.org/en/2013/11/12/situational-report-control-and-censorship-online-media-through-use-laws-and-imposition

iLaw. (2021, December 29). *"New" phenomenon of rights violation in 2021*. Retrieved from https://freedom.ilaw.or.th/node/1009

iLaw. (2022, July 16). *Parasite that smiles: Pegasus spyware targeted dissidents in Thailand*. Retrieved from https://freedom.ilaw.or.th/en/report-parasite-that-smiles

Juodyté, E. (2017, June 22). *Editorial: Thailand*. Nord VPN. Retrieved from https://nordvpn.com/ar/blog/an-overview-surveillance-practices-in-thailand/

Komchadluek. (2020, April 22). Prawit orders to set up anti-fake news and nationwide command centers. Retrieved from https://www.komchadluek.net/news/428278

Lertchoosakul, K. (2021). *Cold war (in) between white ribbons*. Bangkok, Thailand: Matichon Publishing.

Lichbach, M. (1987). Deterrence or escalation? The puzzle of aggregate studies of repression and dissent. *Journal of Conflict Resolution, 31*(2), 266–297.

Mahooney-Norris, K. A. (2000). Political repression: Threat perception and transnational solidarity groups. In C. Davenport (Ed.), *Paths to state repression: Human rights violation and contentious politics* (pp. 71–108). New York, NY: Rowman & Littlefield.

Manager Online. (2021, November 24). Amnesty responds to public pressure. Royalists want it out of the country. Former deputy head of National Intelligence pushes for financial scrutiny. Retrieved from https://mgronline.com/onlinesection/detail/9640000116498

Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance & Society, 16*(2), 219–237. doi:10.24908/ss.v16i2.8346

Marczak, B., Scott-Railton, J., Rao, S. P., Anstis, S., & Deibert, R. (2020, December 1). *Running in circles: Uncovering the clients of cyberespionage firm circles*. Retrieved from https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

Megiddo, T. (2020). Online activism, digital domination, and the rule of trolls: Mapping and theorizing technological oppression by governments. *Columbia Journal of Transnational Law, 85*(2), 394–442. doi:10.2139/ssrn.3459983

Moss, M., Michaelsen, M., & Kennedy, G. (2022). Going after the family: Transnational repression and the proxy punishment of Middle Eastern diasporas. *Global Networks, 22*(4), 735–751. doi:10.1111/glob.12372

Nation TV. (2021, September 17). *Cyber police raided and arrested activist for violating Article 116 and CCA*. Retrieved from https://www.nationtv.tv/news/378840570

Nilkamhaeng, C. K. (2015). Information operations and national security. *Ratthapirak, 58*(3), 71–78.

Ong, J. C., & Cabañes, J. V. A. (2018). *Architects of networked disinformation: Behind the scenes of troll accounts and fake news production in the Philippines*. The Newton Tech4Day Network. Retrieved from https://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1075&context=communication_faculty_pubs

Phanttapak, K. (2021, October 29). *Mapping 112 cases: Citizens filing complaints against citizens*. VoiceTV. Retrieved from https://voicetv.co.th/read/xZ3RycdVl

Prachatai. (2020, February 20). Niranam arrested for violating CCA by tweeting about King Rama 10. Retrieved from https://prachatai.com/journal/2020/02/86426

Prachatai. (2021, June 28). Map of Article 112 violators and THCVC removed after people reported privacy violations. Retrieved from https://prachatai.com/journal/2021/06/93719

Prachatai. (2022, February 22). Monarchy Protection Group alleges a 14-year-old girl of violating Article 112 by reading a petition at the UN. Retrieved from https://prachatai.com/journal/2023/02/102876

Privacy International. (2017, January). *Who's that knocking at my door? Understanding surveillance in Thailand*. Retrieved from https://privacyinternational.org/sites/default/files/2017-10/thailand_2017_0.pdf

Reuters. (2021, November 10). Thai court rules students' royal reform call sought to overthrow monarchy. Retrieved from https://www.reuters.com/world/asia-pacific/thai-court-rules-students-royal-reform-call-sought-overthrow-monarchy-2021-11-10/

Riggs, F. W. (1966). *Thailand: The modernization of a bureaucratic polity*. Honolulu, HI: East-West Center Press.

Royal Gazette. (2007). Computer-Related Crimes Act, B.E. 2550 (2007), No. 124, Sect. 27 kor. Retrieved from https://www.tsu.ac.th/files/Computer_Crimes_Act_B.E._2550_Thai.pdf

Royal Gazette. (2017). (Amended) Computer-Related Crimes Act, B.E. 2560 (2017), No. 134, Sect. 10 kor. Retrieved from http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF

Royal Gazette. (2019a). Cybersecurity Act, B.E. 2562 (2019), No. 136, Sect. 69 kor. Retrieved from http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF

Royal Gazette. (2019b). National Intelligence Act., B.E. 2562 (2019), No. 136, Sect. 50 kor. Retrieved from http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/050/T_0022.PDF

Ruijgrok, K. (2021). The authoritarian practice of issuing internet shutdowns in India: The Bharatiya Janata Party's direct and indirect responsibility. *Democratization, 29*(4), 611–633. doi:10.1080/13510347.2021.1993826

Sambandaraksa, D. (2016, January 26). *Thailand embarks on mass surveillance on social media*. Telecom Asia. Retrieved from https://www.telecomasia.net/content/thailand-embarks-mass-surveillance-social-media/

Siamrath. (2022, March 19). Dr. Seri criticizes nation haters' claims their arrests are due to holding different opinion, but in fact they are foreign agents. Retrieved from https://siamrath.co.th/n/332435

Sombatpoonsiri, J. (2022a). *Labeling "fake news": The politics of regulating disinformation in Thailand*. Perspective 2022/34. ISEAS Yusof-Ishak Institute. Retrieved from https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-34-labelling-fake-news-the-politics-of-regulating-disinformation-in-thailand-by-janjira-sombatpoonsiri/

Sombatpoonsiri, J. (2022b). *"We are independent trolls": The efficacy of royalist digital activism in Thailand*. Perspective 2022/1. ISEAS Yusof-Ishak Institute. Retrieved from https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-1-we-are-independent-trolls-the-efficacy-of-royalist-digital-activism-in-thailand-by-janjira-sombatpoonsiri/

Sombatpoonsiri, J., & An Loung, D. N. (2022). *Justifying digital repression via "fighting fake news": A study of four Southeast Asian autocracies*. Singapore: ISEAS Yusof-Ishak Institute. Retrieved from https://bookshop.iseas.edu.sg/publication/7811

Sombatpoonsiri, J., & Kri-aksorn, T. (2021). Taking back civic space: Nonviolent protests and pushbacks against autocratic restrictions in Thailand. *PROTEST, 1*(1), 80–108. doi:10.1163/2667372X-bja10006

Statista. (2023). *The number of social network users in Thailand from 2017–2020 with a forecast through 2026*. Retrieved from https://www.statista.com/statistics/489230/number-of-social-network-users-in-thailand/

The Straits Times. (2020, January 10). Thais turn to Twitter to criticise royalty. Retrieved from https://www.straitstimes.com/asia/se-asia/thais-turn-to-twitter-to-criticise-royalty

Thai Move Institute. (2020a, November 29). *Dr. Wetin trashes Puangthong's logic defending thieves who stole from the palace*. Retrieved from https://www.thaimoveinstitute.com/37503/

Thai Move Institute. (2020b, August 10). *The (imaginative) people's revolution plot: Simple guide*. Retrieved from https://www.facebook.com/thaimoveinstitute/posts/337175887665731/

Thai Post. (2022, February 11). 1.2 million signatures submitted to evict Amnesty Thailand on 17 February. Retrieved from https://www.thaipost.net/one-newspaper/83140/

Thailand Human Rights Lawyers (TLHR). (2022, June 21). *Arnon Nampa's 12th Article 112 charge after posting #CitizensMessages on November 2020*. Retrieved from https://tlhr2014.com/archives/45076

Thailand Human Rights Lawyers (TLHR). (2023, March 3). *Numbers of those charged with Article 112, from 24 November 2020 to 27 February 2023*. Retrieved from https://tlhr2014.com/archives/23983

Thomas, E., Beattie, T., & Zhang, A. (2020, December). *#WhatsHappeningInThailand: The power dynamics of Thailand's digital activism*. Australian Strategic Policy Institute. Retrieved from https://www.aspi.org.au/report/whatshappeninginthailand-power-dynamics-thailands-digital-activism

Top News. (2021, July 10). THCVC submits evidence to cyber police, accusing more than 1,000 for offending the monarchy. Retrieved from https://www.facebook.com/TopNewsLiveThailand/videos/1790292574485089

The Truth. (2021a, November 19). Amnesty incites people to write 1m letters, defending activist leader and pressuring authorities on charging Rung. Retrieved from https://www.youtube.com/watch?v=IW62fCv2BTI

The Truth. (2021b, October 11). Pao iLaw caught in saying he receives foreign money. Social media users suspect he is hired to overthrow the monarchy. Retrieved from https://truthforyou.co/70289/?anm=

The Truth. (2021c, December 2). Plaew si ngen exposes Rung tricked by US-funded evil movement that operates from university campuses through Thai professors. Retrieved from https://truthforyou.co/77867/

The Truth. (2022, February 23). Thammasat professor criticized for making baseless claims about bail money too hefty. Retrieved from https://truthforyou.co/88687/

Wikileaks. (2013). *Hacking team*. Retrieved from https://search.wikileaks.org/advanced?q=Thailand+&exclude_words=&words_title_only=&words_content_only=&publication_type%5b%5d=36&publication_type%5b%5d=37&sort=0#results

Wilson, R. A. (2022). The anti-human rights machine: Digital authoritarianism and the global assault on human rights. *Human Rights Quarterly, 44*(4), 704–739. doi:10.1353/hrq.2022.0043

Wongcha-um, P., & Johnson, K. (2020, December 18). *The last taboo: A new generation of Thais is defying the monarchy*. A Reuters Special Report. Retrieved from www.reuters.com/investigates/special-report/thailand-protests-youth/

Zuboff, S. (2019). *The age of surveillance capitalism: The flight for a human future at the new frontier of power*. London, UK: Prolific Books.