POLICING CYBERSPACE: UNDERSTANDING ONLINE REPRESSION IN THAILAND AND THE PHILIPPINES

Fernan Talamayan

Institute of Social Research and Cultural Studies, National Chiao Tung University, Taiwan
ftalamayan.srcs07g@nctu.edu.tw

Received: 25th October 2020/ **Revised:** 07th November 2020/ **Accepted:** 28th November 2020

How to Cite: Talamayan, F. (2020). Policing cyberspace: Understanding online repression in Thailand and the Philippines. *Journal of ASEAN Studies, 8*(2), 129-145.

https:/doi.org/10.21512/jas.v8i2.6769

ABSTRACT

Social networking sites have become increasingly relevant in the study of democracy and culture in recent years. This study explores the interconnectedness of social networks, the imposition of state control, and management of social behavior by comparing various literature on the operation of repression in Thai and Philippine cyberspaces. It examines the overt and covert policing of daily interactions in digital environments and unpacks governmental technologies' disciplinary mechanisms following Michel Foucault's notion of government and biopolitical power. Subjugation in the context of social networks merits analysis for it sheds light on the practice of active and passive self-censorship—the former driven by the pursuit of a moral self-image and the latter by state-sponsored fear. In tracing various points of convergence and divergence in the practice of cyber control in Thailand and the Philippines, the study found newer domains of regulation of social behavior applicable to today's democracies.

Keywords: *cyberspace, algorithm, policing, online repression, self-censorship*

INTRODUCTION

According to Habermas (2006), political communication on the internet claims "unequivocal democratic merits" in the context of undermining censorship of authoritarian regimes (p. 423). Quite the contrary, it could be observed that in nations like Thailand and the Philippines, the internet has been instrumental in silencing dissent or harassing or jailing opposition members. While the internet has long been regarded as a facilitator of democracy (Benkler, 2006; Gillmor, 2004; Grossman, 1995; Rheingold, 1993/2000) and a platform for political discourse (Poster, 1997 in Geiger, 2009), it has also been utilized by authoritarian and

authoritarian-like governments as an instrument to suppress people's freedom (Sombatpoonsiri, 2018) and exert hegemonic control in cyberspace (Frechette, 2005; Laungaramsri, 2016; Schaffar, 2016; Sinpeng, 2013). The motivations and objectives of these governments may vary, but the exercise of hegemony and the operation of repression are relatively similar. Mainly, in their attempts to dictate the political discourse in "digital public spheres" (Hearn, 2010; Macnamara, 2008; Mahlouly, 2013; Valtysson, 2012), such regimes instigate fear or assert a peculiar sense of morality to manage citizen behavior and police information flows.

This study surveys the current scholarship on Thailand and the Philippines, where the incidence of cyber repression and manipulation has increased at an alarming rate in recent years. As both Thailand and the Philippines are suffering from disinformation and extreme polarization, these countries are interesting case studies in understanding the operation of online repression in democratic states in Southeast Asia. In comparing their experiences, the study elaborates on how various scholars identify the roles of the authorities (military junta in Thailand and the Rodrigo Duterte administration in the Philippines) and their supporters in the development of new and more efficient forms of cyber control. It discusses the activities of the Thai junta's Cyber Scouts and Duterte's keyboard army in an attempt to compare and unravel the systematic operation of hegemonic control in these two countries' cyberspace.

The study raises the following questions: How does the internet become instrumental in the reproduction of the state's domination over individuals' daily affairs? What are the tools and techniques that authoritarian regimes use in patrolling and controlling cyberspace? How is normative power exercised in cyberspace? How does cyber trolling and harassment influence the governance of the self and others? These questions will be answered following Michel Foucault's concept of government and biopolitical power while employing a comparative approach to establish and analyze the essential systemic features of governmental and political interventions in contemporary digital spaces.

LITERATURE REVIEW

This research extends Sombatpoonsiri's (2018) exploration, which compared the Thai and Philippine governments' strategies of political repression and cyber control. Observing the striking similarities in the internet regime and political situation in Thailand and the Philippines, she explained how autocratic and illiberal regimes exploit existing social divides to consolidate power. She argued that the government's instrumentalization of cyberbullying is a manifestation of the deeper crisis of social polarization. Complementing her analysis on the correlation between the crises of polarization and governments' mobilization of the public in controlling cyberspace, this study refers to Sombatpoonsiri's described forms of political repression as governmental techniques that conduct people's conduct in digital environments.

Similarly, recognizing the vulnerability of democracy under authoritarian regimes, Sinpeng (2013) zeroed in on Thailand's internet regime (p. 421) as she examined the role of

the internet in the entrenchment of democracy. Sinpeng questioned the internet's democratizing role in the cyber era, positing that the internet serves as a tool for repression through state online coercion, as was the case in Thailand. Along these lines, Laungaramsri (2016) tackled Thailand's "troubling" shift toward censorship, surveillance, and suppression in cyberspace. Drawing on Foucault's "governmentality," she described the normalization of surveillance in post-coup Thailand through the politicization, securitization, and militarization of the internet by the Thai junta. Meanwhile, Ramasoota (2016) touched on cyber-witch hunting in Thailand in the post-2014 coup as she elaborated on how cyber-witch hunters harass people with differing views and undermine their privacy rights.

Despite the absence of cyber-witch hunts and anti-royalism in the Philippines, the promotion of fear and the exercise of hegemonic control of an authoritarian-like regime such as Duterte's also threaten freedom of expression and privacy rights. Incidence of cyber trolling and harassment of political opposition in the Philippines has increased dramatically since Duterte's assumption of the presidency. Ong and Cabañes (2018) pointed out that many Filipinos who expressed disgust towards Duterte were repeatedly hounded and harassed with the use of negative speeches, expletives, and death threats. Whereas the research of Ong and Cabañes explained the "moral justification in the disinformation project" (pp. 29-30, see also Ong & Cabañes, 2019) and impressed how cyber trolling has become a tool for cyber manipulation and control, most noteworthy is their effort to expose the existence of an industry responsible for the manipulation of algorithms of online platforms, which help the promotion of political propagandas in the Philippines.

While this study often refers to the works of the previous researchers throughout its discussion, it simultaneously deviates by suggesting categories in which the described coercive activities could be plotted. By making apparent the characteristics of identified repressive actions, the study determines the type of technology that a state and its supporters execute to govern and influence groups and individuals, such as algorithmic gatekeeping, algorithmic policing, and cyber policing. As an art of government, these technologies are often employed synchronously whenever possible.

In the next sections, the study briefly explains Foucault's notion of biopolitical power, which is mobilized as a conceptual tool to analyze internet regimes and the practice of government in Thailand and the Philippines. This concept acts as a bridge that links governmentality with new technologies of policing (algorithmic gatekeeping, algorithmic and cyber policing). These technologies exploit the vulnerabilities of social network designs by manipulating the flow of information and discourse on the internet. To adequately describe these new technologies of government, the supposed democratizing effect of the internet is questioned as it explains how the "illusion" of freedom is manufactured through and within the internet's internal and external logic.

ANALYTICAL FRAMEWORK

The supposedly "mutually beneficial" arrangement between citizens and the state (controlling the population to foster both citizen's life and the state's strength) introduced the paradigm of biopolitical power (Foucault, 1981, pp. 248-252). The goal of biopolitical power is to optimize and multiply life by subjecting it to precise controls and comprehensive regulations (Foucault, 1978, p. 137). This kind of power is exercised through constant supervision of its subjects (the individual). Individuals regularly police themselves and others by examining and controlling their and other people's thoughts and behavior in accordance with what society has constructed as the norm (Bevir, 1999, p. 65). With the birth of biopolitical power, social norms have become a critical regulator of people's communication and daily activities. Moreover, with the promise of the society to secure life and happiness, people subject themselves to such power.

The society's essence gives teeth to biopolitical power. In describing the intrinsic nature of the society, John Stuart Mill (1859/2003, p. 139) wrote:

> Though society is not founded on a contract, and though no good purpose is answered by inventing a contract in order to deduce social obligations from it, everyone who receives protection of society owes a return for the benefit, and the fact of living in society renders it indispensable that each should be bound to observe a certain line of conduct towards the rest.

The idea that one is bound to observe a certain conduct towards the rest gives the society the authority to conduct the conduct of an individual. Mill (1859/2003) added that society is granted jurisdiction over a person's behavior, especially when it prejudicially affects other people's interests (p. 139). Because of this jurisdiction, individuals are expected to discipline themselves and act following the norms.

This arrangement between the individual and society would also have an impact on the construction of the moral self-image, since morality is understood as "the attempt to make oneself accountable for one's own actions" (Dean, 1999/2010, p. 19). Self-regulation is treated as a moral activity, as the practice of government is presumed to know "what constitutes good, virtuous, appropriate, responsible conduct of individuals and collectives" (p. 19). That said, conducting other people's conduct becomes a moral activity too. This explains why public opinion, which is presumed to constitute ethical principles, is used to regulate, or in some cases, punish individuals who, for instance, have dissenting and opposing views.

In other words, government is the "conduct of conduct" (Foucault, 1982, pp. 220-221 in Dean, 1999/2010, p. 17). The different meanings of conduct imply some sort of calculation as to how government is carried out. It also influences today's understanding of self-control or self-regulation, as conduct in this framework involves conducting oneself (pp. 17-18). To govern is to manage human behavior via social norms, structure the field of possible action, and act on individuals' capacities for action (p. 22). In this light, an actor's (state or supporters)

exploitation of digital platforms' architecture and manipulation of social media algorithms play a significant role in shaping human behavior and delimiting social interaction.

Meanwhile, it is the law that gives programs and technologies its coercive power (Foucault, 1978/2001, p. 232). Although Foucault was originally referring to the programs in educational, medical, and military institutions when describing the relationship between law, power, program, and technologies, it can be argued that the same principles may apply in digital spaces. Social media users are similarly subjected to coercive measures that follow sets of calculated prescriptions (i.e., algorithms and software designs), arranged spaces (i.e., filters, sitemaps, or firewalls), and regulated behaviors (i.e., website's privacy policies or terms of service that govern the use of a digital platform). Additionally, these sets of rules are stacked on top of laws and state policies that govern citizens.

RESEARCH METHOD

Apart from conducting a survey of literature that reflects on the state of democracies in Thailand and the Philippines, the author gathered empirical evidence from various Facebook pages of public figures (or of those supporting and promoting public figures) such as Duterte's *Duterte Media, Duterte sa Pagbabago Bukas (Duterte for Tomorrow's Change), Duterte Diehard Supporters (DDS),*[1] *Duterte Phenomenon*, *Pinoy Monkey Pride, Thinking Pinoy, Mocha Uson Blog, DU30 Trending News,* or pro-junta's platforms such as *The New Atlas, Alt Thai News Network,* and *New Eastern Outlook.*[2] As a qualitative research, the author treated these online groups and platforms as his field and employed purposeful sampling to provide "information-rich cases" (Patton, 2005, p. 2). Immersion in these groups involved observation of several state supporters' posts and activities. The author also analyzed the content and comment section of several YouTube videos that promoted the state's agenda. To discover various pro-state channels, the author followed the recommendations on YouTube, as they often suggest similar contents and channels.

ANALYSIS

This section compares several scholars' discussion on how people's conduct is conducted in the Thai and Philippine cyberspaces. In navigating various works, this study intervenes by hinting on digital governmental techniques that are observably practiced by authoritarian regimes such as algorithmic gatekeeping, algorithmic policing, and cyber policing. To understand these technologies, it is imperative to introduce what an algorithm is and describe what it can do.

Algorithms are sets of instructions designed to perform specific tasks or operations efficiently. Offering a more critical definition, Tufekci (2015) describes algorithms as "computational processes that are used to make decisions of such complexity that inputs and

outputs are neither transparent nor obvious to the casual human observer" (p. 206). While some computational processes involve simple operations such as multiplication of numbers, issues could be raised on other algorithms that involve "subjective decision making" wherein no single correct answer could be determined (pp. 206-207). In the context of digital journalism, algorithms affect the selecting, sorting, and ordering of news (Carlson, 2017, p. 2). It also prioritizes and shapes the content that becomes visible to the people.

In environments where popularity drives the production of contents and personalization is valued over mass messaging (Carlson, 2017, p. 7), relevance becomes critical in determining algorithmic calculations. As tech giants present social networking sites as spaces that individuals could control through the logic of relevance, these sites give an impression to their users that one could curate their news feed, block contents that they deem foul or obscene, or follow and share stories which they consider informative or entertaining. However, it must be noted that what becomes relevant to the public may be influenced by what is presented or offered to them. Hence, when algorithmic manipulation limits content selection, what becomes relevant to social media users become regulated without the public's knowledge. This lack of visibility of algorithmic decisions reinforces the "illusion" of freedom appropriated to and by the people. It is this lack of visibility of algorithms that makes social media users vulnerable to manipulation. The maneuvering of internet content, as well as the discourse in the said platform, in effect, creates an illusion of choices as choices become pre-determined by an algorithm. Tufekci (2015) notes that such manipulations are performed routinely in many online platforms. She writes, "they range from purposes as mundane as deciding the color of a button, to decisions as which news article is shown to the public" (p. 205).

The regulation of digital content consumed by the public is carried out through algorithmic gatekeeping and algorithmic policing. Tufekci (2015) defines algorithmic gatekeeping as "the process by which transparent algorithmic computational-tools dynamically filter, highlight, suppress, or otherwise play an editorial role…in determining information flows through online platforms and similar media" (pp. 207-208). Algorithmic gatekeeping is instrumental in managing public opinion, for it helps actors control political communication and meaning-making processes through algorithmically driven filters. On the other hand, algorithmic policing is used as a formal apparatus of control (Norris, 2008), which involves big data surveillance tasked to predict risks and future crimes (Brayne, 2017).

Several Facebook pages and communities contribute largely to the algorithmic gatekeeping and policing of the Philippine and Thai cyberspaces. Like-minded Filipino supporters of Duterte gather in Facebook pages of public figures (or of those supporting and promoting public figures) such as Duterte's *Duterte Media, Duterte sa Pagbabago Bukas* (Duterte for Tomorrow's Change), *Duterte Diehard Supporters, Pinoy Monkey Pride, Thinking Pinoy* and *DU30 Trending News,*—together they disseminate content that supports Duterte's policy decisions and actions. Similarly, the case in Thailand is where the right-wing and anti-liberal online media such as *T-News, Chaophraya News, Deep News, The New Atlas, Alt Thai News Network* and *New Eastern Outlook* align their content and activities with those of the

cyber scouts, Garbage Collector Organization (GCO), and the military junta (Sombatpoonsiri, 2018, p. 4). Following the logic of social media algorithms, the government, social media influencers, and supporters' (Duterte's DDS in the Philippines and the pro-junta online media in Thailand) combined effort would have, in theory, an impact on their countries' information flows. The sheer volume and frequency of the production and proliferation of pro-Duterte and pro-junta contents would have influenced the computational processes of these sites and created a sense of relevance in various social media's programming language. Facebook's banning of fake accounts linked to pro-state groups and the military in 2019 (Thailand) and 2020 (Philippines) provides clues on the potential influence of algorithmic gatekeeping and policing on people's activities and behavior in digital platforms.

Social politics curation or the practice of curating news and political content on social networking sites (Thorson, 2014, p. 207) has become instrumental in exercising algorithmic manipulation in the Philippines. A number of celebrities and bloggers like Mocha Uson (a former singer-dancer and a current appointive public official), RJ Nieto (the author of the pro-Duterte Facebook page *Thinking Pinoy*), Mark Lopez (a pro-Duterte blogger), and many others who have large followings have taken the lead in curating news in the Philippines. Reports show (see *VERA Files Year-ender Report 2017*) that their active sharing and distribution of content that support and venerate Duterte have sustained the generation of likes for such posts. Duterte's keyboard army and supporters backed these social media influencers. Believing that Duterte is the "leader that Filipinos need" (Maboloc, 2018, p. 93), they "willingly" participate in spreading pro-Duterte content on the internet, regardless of the content's credibility.[3] Further, Duterte's cyber troops have been relentless in attacking his critics, particularly those who oppose the government's war on drugs, which has claimed thousands of lives through extrajudicial killings (Sombatpoonsiri, 2018, p. 3).

Although most celebrities, bloggers, or other fervent supporters of the Duterte administration claim that they act on their own accord, Ong and Cabañes (2018) expose the existence of an institutionalized network of disinformation that guides them by explaining how politicians utilized this network to influence digital platforms' algorithms. They also report that in its operation, "high-level strategists operators pass on the 24/7 running of these accounts (Facebook fake accounts) to lower-level account operators" (Ong & Cabañes, 2018, p. 50). Multiple fake social media accounts are used in their operation to amplify their propaganda and ensure a "high degree of algorithmic visibility, as they can maintain intense interactivity and engagement with their followers and supporters" (pp. 37, 50). These accounts often manifest "inauthentic behavior," defined by Facebook as the use of deceptive behaviors to conceal an organization's identity, making the organization and its campaign seem "more popular or trustworthy" than it actually is (Gleicher, 2019).

As propaganda becomes highly visible in digital platforms, the more it can "hook" or "capture" users. This is possible through political actors' constant production of propagandistic materials and social media's internal computational processes that help users further immerse in materials and contents related to what they click on their feed. Since algorithms assume its

users' choices and behavior, users who interact with a particular content may end up seeing more of that material. Once users become "captives" of both the platform and certain content, it is highly likely that the social networking site, guided by its algorithm, would direct them to other videos and threads with similar content. For instance, if a YouTube user who has just started following a propaganda lets YouTube's autoplay function work, the platform will decide to immerse that user in more videos that it deems relevant. YouTube also has a mechanism that remembers watched videos. Suggestions and updates based on viewing history welcome a user when they reopen the platform. This design makes it convenient for pro-Duterte vloggers to promote pro-Duterte content as the platform helps them reach out to and update their audience. YouTube's relevance, ranking, and search algorithms can also induce the repetition of key propaganda messages. This repetition helps propaganda become the "truth" to propaganda believers, and this "truth" is instrumental in influencing how they pass judgment on others.

While this study highlights certain actors' manipulation of algorithms to affect people's moral compass, attention must be given to media content production, especially since media content also drives faithful readership or viewership. Several audio-visual materials from Pro-Duterte bloggers use the vernacular of the "people" (by "people" the study pertains to the supporters of Duterte). Their tone is often conversational, and their choices of words appeal to the ordinary Filipino, as they employ common street language and even profanity on some occasions (see the regular posts of Mr. Riyoh, Banat By, Mark Lopez, etc.). They also sound as if they represent the Filipino people, providing their people with a voice that has long been silenced or neglected by technocrats or reformists. Their videos follow Duterte's "anti-establishment strategy" (Maboloc, 2019, p. 170) and follow an "us-versus-them" narrative, a characteristic familiar to populist rhetorical styles. These political communication techniques make some of their followers assert that their likes should reclaim "power" from the educated and landed elite. More importantly, the repetition and multiplication of such political content aid in transforming propaganda into a "basic grammar" (Vatsov, 2018, p. 77) that frames state supporters' articulation of moral intuitions.

Another form of policing that has gained popularity in contemporary authoritarian regimes is what several scholars refer to as cyber policing (Ramasoota, 2016; Sinpeng, 2013; Sombatpoonsiri, 2018). What distinguishes cyber policing from algorithmic policing is its overtness—while the latter operates outside the conscious, that is, often stealthy and invisible (Tufekci, 2015, pp. 208-209), the former allows itself to be known to instigate fear. Cyber policing also involves the policing of information flows by controlling citizens' behavior (Sinpeng, 2013, p. 423). This mode of policing is often supported and normalized by the state through legislation or state policies. In other contexts, the head of state's public statements could also promote the normalization of cyber policing, for, in such places, people may regard every word uttered by the head of state as the policy of the state. As such, cyber policing may enforce self-censorship. The promotion of self-censorship in cyberspace is further discussed in the subsequent paragraphs.

Thailand's Cyber Scout Program and cyber-witch hunting are examples of what the study pertains to as cyber policing. According to Laungaramsri (2016), the initiation of the Cyber Scout Program and cyber-witch hunt and the junta's employment of deceptive tactics curtails freedom of expression in Thailand (pp. 195-204). Observing the practice of cyber policing in Thailand, the Computer Crime Act (CCA) in 2007 and Article 112 or the lèse-majesté act of the Thai Penal Code provide guidelines (or "programs") that inform individual behavior. Apart from acting as "grids for the perception and evaluation of things" (Foucault, 1978/2001, p. 232), they also create a blueprint that dictates how society should regulate its people in Thai cyberspace. Briefly, the CCA of 2007 legalizes the blocking of internet content by the government, and it makes internet content providers liable for any direct or indirect violations (Ramasoota, 2011 in Sinpeng, 2013, p. 428). It also legalizes the infringement of people's right to privacy, as the law permits the exposure of the identities of internet users without the users' consent (p. 428). Sinpeng notes that this law does not provide clarity as to what exactly it specifies as a crime and any actions committed online, which the government deems as a threat to national security could be legally charged (pp. 428-429). Article 112 or the lèse-majesté act, on the other hand, prohibits defamation, insults or threats to the King, the Queen, the Heir-apparent, or the Regent. Violators of Article 112 could face three to fifteen years of imprisonment for each count of offense (Ramasoota, 2016, p. 271). Needless to say, these laws serve as regulatory mechanisms in directing people's offline and online activities and behavior. These laws empower the Cyber Scouts, and they also serve as the driving force behind several cases of cyber-witch hunting in Thailand.

The Cyber Scout Program is a project initiative of the royalist-conservative government of Abhisit Vajjajiva that professionalized online royalist vigilante groups in Thailand (Schaffar, 2016, p. 224). It established the organization called the Cyber Scout Thailand, which was set up to "create ethical and moral online conduct and ensure the creative and appropriate use of information, communication and technology" (cyberscout.in.th). The members of this program, called Cyber Scouts, are given instructions on the historical significance of the monarchy, as well as the cyber laws and ethics, and are provided with technical training (Schaffar, 2016, p. 224; Sinpeng, 2013, p. 432). They work undercover to befriend suspects on Facebook, start conversations about sensitive issues, patrol cyberspace, and report violators of the lèse-majesté to the authorities (Schaffar, 2016).

It is important to note that while Thailand's Ministry of Information and Communication Technology (MICT) supports these Cyber Scouts, the members participate voluntarily (Ramasoota, 2016, pp. 273-274). Volunteerism, in this context, appeals to people's sense of morality. Activities such as identifying and locating violators of the CCA of 2007 and Article 112 are perceived as altruistic, as they are deemed to contribute to the reduction of nonconformity and social tensions. Moreover, these volunteers work in incognito mode (invisible to others). Since anyone, such as friends or colleagues, can be a Cyber Scout, it encourages people to be careful with whatever they do or post online. Hence, apart from the laws' vagueness regarding what the state deems punishable, knowledge about Cyber Scout's

existence potentially creates a cloud of fear. In such a context, fear becomes a fundamental tool in governing the self and others.

Another Thai organization that monitored people's behavior on the internet for the purpose of protecting the monarchy is the self-proclaimed ultra-royalist Garbage Collector Organization (GCO). Founded by Major General Rienthong Nanna, a retired medical doctor and a director of Mongkotwattana Hospital, the GCO derived its name from the idea that people expressing contrary views are trash (Stapleton, 2015 in Ramasoota, 2016, p. 276). Schaffar (2016) states it is an organization of ordinary people from the streets who participate in cyber-witch hunting, or the reproaching and public lynching of "social rebels or those expressing non-conforming views online" through the circulation of the nonconformists' "unorthodox attitudes" to the "conforming community" on the internet (Ramasoota, 2016, p. 269). Their activities included the public humiliation and pacification of the supporters and business partners of the exiled Prime Minister Thaksin whom the people refer to as the Red Shirts (Schaffar, 2016). They also collectively campaigned to expose violations of lèse-majesté. The GCO's cyber-witch hunt activities were considered more threatening since they involved privacy rights violations and offline mobbing.

Cyber-witch hunt undermines Thai citizens' privacy rights through doxxing, defined as the hacker's habit of collecting personal and private information to be released publicly against a person's wishes (Ramasoota, 2016, p. 273). GCO's activities often involved doxxing. A well-documented example of such is the case of a Red Shirt activist, Tananun Buranasiri. The GCO disclosed Tananun Buranasiri and her family's personal information to the public after she posted comments that are perceived as violating Article 112. The disclosed information included the location of her workplace, and when the mob started appearing in front of her workplace, her employer decided to fire her. The misfortune of Tananun Buranasiri did not end with the termination of her employment as the GCO unrelentingly harassed her online by "insulting her and exchanging fantasies about how to 'get rid' of her" (Schaffar, 2016, p. 216).

Other pro-monarchy political groups such as the Seri Thai Movement, Thai Netizen Network, and the People's Alliance for Democracy movement encourage their members to participate in the policing of the Thai cyberspace by reporting online violators of lèse-majesté to MICT. In 2012 the Thai Free News reported that the People's Alliance for Democracy movement alone was responsible for "filing 16 complaints accusing individuals, including some high-profile journalists, of committing computer crimes" (Sinpeng, 2013, p. 432).

In the Philippines, it is in the network disinformation described by Ong and Cabañes that cyberbullying and trolling, which are more subtle forms of cyber policing (compared to Thailand), are exercised. It is, in a sense, the modern form of Foucault's "government of men by men." Cyber trolling police people in several ways. For instance, Filipinos who express opposing views in public Facebook pages are repeatedly hounded and harassed by Duterte's keyboard army not only through negative speech or expletives but also death threats (Ong & Cabañes, 2018, p. 13). Amplification of pro-Duterte messages by both Duterte supporters and

troll accounts also creates a sense of "public consensus" in threads that touch upon controversial political issues. It is also a common practice to attack "nonconformists" by appealing to people's morality and "patriotism;" Pro-Duterte accounts, for example, accuse Duterte's critics as evil, self-centered, elitist, anti-Filipino, or anti-progress. There are also instances when they would just repeatedly dismiss dissent as "stupid," "ignorant," or "misinformed."

The way the keyboard army attacks and silences Duterte's critics are easily comparable with how Thailand's GCO conducts cyber-mobbing. Both groups are notorious for their usage of indecent language and offensive speech. Stemming their strength from the grassroots, they fearlessly harass non-conforming people all in the name of defending their respective champions. The activities of these cyber trolls promote self-regulation among social media users, especially to those who wish to spare themselves the trouble of engaging or being harassed by the Duterte or Thai junta supporters. This form of cyber policing could enforce self-censorship as it encourages individuals to discipline and control their thoughts and actions to avoid state punishment or societal judgment.

There are, however, fundamental differences between the two. Since the type of authoritarianism in Thailand and the Philippines varies, the type of supporters and the policing activities will also vary. Arguably, Duterte enjoys a rather stable popular support while the Thai regime relies heavily on many autocratic techniques to remain in power. As a result, Duterte's keyboard army shows no interest in cracking down or spying on their targets, unlike the Thai cyber scouts or GCO. Keyboard armies focus their energy on silencing political enemies and spreading disinformation to gain greater support and attract more followers. Meanwhile, Thailand's GCO has been known for infiltrating anti-monarchy pages to search and destroy anti-monarchists. They pretend to insult the monarchy to provoke similar action (Ramasoota, 2016, p. 279) and ultimately identify those who violate the lèse-majesté. In Foucauldian terms, these fundamental differences manifest the specific regularities, logic, strategy, and reason for distinct regimes of practices.

As exhibited by the practices of online policing in Thailand and the Philippines, the seemingly overwhelming presence of cyber scouts and trolls and their constant harassment of the "enemies" of the state contribute to the normalization and legitimization of repression in cyberspace. In the case of Thailand, its transitioning back to democracy paved the way for the reinforcement of increased censorship and control over the internet through legislation and cyber policing. The government's imposition of harsh penalties for violating internet-related laws and their supporters' active collaboration in identifying and harassing nonconformist citizens has resulted in greater self-censorship in online discussions (Sinpeng, 2013, p. 429). The domination in social networking sites of Duterte's keyboard army and other supporters, whose activities were directed at manipulating social media algorithms and shaping public opinion in favor of the current Philippine administration, has discredited and silenced dissent (Ong & Cabañes, 2018, p. 3). Like the Cyber Scouts or GCOs, the actions of Duterte's keyboard army may promote self-regulation, especially to those who wish to spare themselves the trouble of engaging or being harassed by the Duterte supporters. In these cases, one would see a

combination of what Foucault (1982/2001) described as "individualization techniques" and "totalization procedures" (p. 332).

The stories of cyber repression and "patriotic" trolling in Thailand and the Philippines show that cyber control, as a technology of government, conducts people's conduct. Following Foucault's concept of "government of men by men," the idea that it is the responsibility of every Thai citizen to respect the monarchy and uphold the agenda of the state transfers the responsibility of policing individuals to individuals. It becomes the responsibility of every Filipino to protect and defend the president and his administration from "destabilizers" and "detractors."

CONCLUSIONS

In examining the practice of censorship and control in contemporary cyberspace, the study compared existing literature on Thailand and the Philippines, as both have been particularly active in exercising newer forms of surveillance and political repression on the internet. Since power in this context operates in digital environments, the exercise of policing requires new techniques of administering and maneuvering. New governmental technologies such as algorithmic gatekeeping, algorithmic policing, and cyber policing are utilized by different agents to instigate fear, engineer public consensus, and control people's activities and behavior.

This study reassessed the current scholarship on Thai and Philippine cyber control by highlighting the intersection of political actors (state and supporters), state policies, and social networks. It argued that the relationship between the three framed the nature and structure of policing practices in Thai and Philippine cyberspaces. The study also intervened by demonstrating how varying forms of autocracy affect the modes of governing the population. In this regard, Foucault's notions of government and biopolitical power were operationalized to flesh out fundamental differences between the regimes of practices in Thailand and the Philippines.

In Thailand, the literature showed that mass surveillance is conducted to maintain the order prescribed by the state (Laungaramsri, 2016, p. 209). The violation of people's privacy rights was done in the name of "protecting" the national security, and the enactment of pro-junta and pro-monarchy cyber-related laws and the normalization of spying and cyberbullying on the internet were legitimized by a peculiar sense of morality. Citizens were encouraged to patrol cyberspace and take part in the activities of organizations that have aligned their objectives and ideals with the state. In the Philippines, despite the lack of strict cybercrime laws, repression is similarly promoted through algorithmic gatekeeping and cyber trolling. The so-called network of disinformation architected by the camp of Duterte (or by his followers) has been very active in maneuvering internet traffic and silencing dissent as it takes advantage of the current incapability of the Philippines to identify online trolls who use fictitious names.

State supporters' apprehension of others and their projection of virtuous self-image are done in the name of "patriotism," morality, and progress. Note, however, that despite comparing the situation in Thai and Philippine cyberspaces, the study does not claim that the above-mentioned autocratic practices are exclusive to both countries. In fact, they can be perceived as symptoms of the general decline in internet freedom among the member states of the Association of Southeast Asian Nations (ASEAN).

As Foucault reminds, government does not only pertain to the political structures or management of states. Instead, it defines or directs the way individuals or groups conduct and behave themselves (Foucault, 1982 in Felluga, 2015, p. 121). Surely, with an ever-increasing number of citizens who become active participants on social networking sites, it would make sense for governments to adopt new techniques and rethink how it would govern its people. While new technologies affect and transform daily life, new regulatory and ideational mechanisms persistently control social behaviors. And with the evolution of technology, the techniques of policing become more comprehensive and penetrating.

The regulatory and ideational mechanisms of such technologies allow for the manipulation of public consensus in digital communities. Capitalizing on the existing social divide in Thailand and the Philippines, both governments have effectively used the us-versus-them perspective and mobilized people's sentiments to promote their brand of totalitarianism. Admittedly though, observing glimpses of resistance and identifying the apparent systemic features of governmental and political interventions in cyberspace may not necessarily solve the host of issues that surround it. Nevertheless, unraveling the fundamental nature of government and policing in the context of today's internet is a start.

Notes

[1]DDS derives its name from the Davao Death Squad, the infamous vigilante group in Duterte's hometown known for committing extrajudicial killings.

[2]In 2019, Facebook removed 12 social media accounts and 10 pages linked to the *New Eastern Outlook* and *The New Atlas*. These accounts and pages were removed for using fake accounts, creating fictitious personas, and driving users to "off-platform blogs posing as news outlets" ("Facebook shows posts," 2019).

[3]It is common for the producers of such media texts to claim that they voluntarily publish content that supports the government. An interview conducted by Ong and Cabañes (2018) explains the rationale behind the perceived credibility and morality in volunteerism. As an anonymous Filipino social media influencer informed, it is a must for them to avoid any sign of control in engaging in debates or promoting campaigns in social networking sites. Showing signs of control would potentially result in losing followers, as they become branded as "*bayaran*" or "paid stooge" (p. 36).

ABOUT THE AUTHOR

Fernan Talamayan is a Ph.D. candidate at the Institute of Social Research and Cultural Studies, National Chiao Tung University, Taiwan. He holds Master's degrees in Sociology and Social Anthropology from the Central European University, Hungary (2018) and History from the University of the Philippines Diliman (2014). His dissertation project investigates governmental practices of populist and fascist regimes in social media. He also conducts research on the marginalization of indigenous communities, colonial advertising, historical revisionism, and propaganda.

ACKNOWLEDGMENT

This research was awarded the Empowering Network for International Thai and ASEAN Studies (ENITAS) Research Scholarship 2020 by the Institute of Thai Studies, Chulalongkorn University, Thailand.

REFERENCES

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven and London: Yale University Press.

Bevir, M. (1999). Foucault and critique: Deploying agency against autonomy. *Political Theory*, *27*(1), 65-84. https://www.jstor.org/stable/192161

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, *82*(5), 977-1008. https://doi.org/10.1177/0003122417725865

Carlson, M. (2017). Facebook in the News. *Digital Journalism*, *6*(1), 4-20. https://doi.org/10.1080/21670811.2017.1298044

Dean, M. (2010). *Governmentality: Power and Rule in Modern Society* (2nd Ed.). London: Sage Publications Ltd.

Facebook shows posts of banned accounts in Thailand. (2019, July 26). *Bangkok Post.* https://www.bangkokpost.com/thailand/politics/1719415/facebook-shows-posts-of-banned-accounts-in-thailand

Feldman, G. (2012). *The Migration Apparatus: Security, Labor, and Policymaking in the European Union*. California: Stanford University Press.

Felluga, D. F. (2015). *Critical Theory: The Key Concepts*. Oxon and New York: Routledge.

Foucault, M. (1978). *The history of sexuality*. New York: Pantheon Books.

Foucault, M. (1978/2001). Questions of method. In P. Rabinow & J. D. Faubion (Eds.), *Essential works of Foucault, 1954-1984* (Volume 3, pp. 223-238). New York: New Press.

Foucault, M. (1981). Omnes et singulatim: Towards a criticism of "political reason". In S. McMurrin (Ed.), *The Tanner Lectures on Human Values II*, (pp. 223-254). Salt Lake City: University of Utah Press.

Foucault, M. (1982/2001). The subject and power. In P. Rabinow & J. D. Faubion (Eds.), *Essential works of Foucault, 1954-1984* (Volume 3, pp. 326-348). New York: New Press.

Foucault, M., Senellart, M., Ewald, F., & Fontana, A. (1983/2007). *Security, territory, population: Lectures at the Collège de France, 1977-1978*. New York, N.Y: Picador/Palgrave Macmillan.

Frechette, J. (2005). Cyber-democracy or cyber-hegemony? Exploring the political and economic structures of the internet as an alternative source of information. *Library Trends, 53*(4), 555-575. https://www.ideals.illinois.edu/handle/2142/1748

Geiger, S. R. (2009). Does Habermas understand the Internet? The algorithmic construction of the blogo/public sphere. *Gnovis: A Journal of Communication, Culture, and Technology, 10*(1), 1-29. https://escholarship.org/uc/item/60s6s0p8

Gillmor, D. (2004). We the media: The rise of citizen journalists. *National Civic Review, 93*(3), 58-63. https://doi.org/10.1002/ncr.62

Gleicher, N. (2019, October 21). How we respond to inauthentic behavior on our platforms: policy update. *Facebook.* https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/

Grossman, L. K. (1995). *The Electronic Republic: Reshaping Democracy in the Information Age.* New York: Viking.

Habermas, J. (2006). Political communication in media society: Does democracy still enjoy an epistemic dimension? The impact of normative theory on empirical research. *Communication Theory, 16*, 411-426. https://doi.org/10.1111/j.1468-2885.2006.00280.x

Hearn, A. (2010). Structuring feeling: Web 2.0, online ranking and rating, and the digital "reputation" economy. *Ephemera: Theory and Politics in Organization, 10*, 421-438.

Johnson, A. (2014). Foucault: Critical theory of the police in a neoliberal age. *Theoria, 141*(61), 5-29. https://doi.org/10.3167/th.2014.6114102

Laungaramsri, P. (2016). Mass surveillance and the militarization of cyberspace in post-coup

Thailand. *ASEAS – Austrian Journal of South-East Asian Studies, 9*(2), 195-214. https://doi.org/10.14764/10.ASEAS-2016.2-2

Lemke, T. (2002). Foucault, governmentality, and critique. *Rethinking Marxism: A Journal of Economics, Culture and Society, 14*(3), 49-64. https://doi.org/10.1080/089356902101242288

Maboloc, C. R. (2018). The radical politics of nation-states: The case of President Rodrigo Duterte. *Journal of ASEAN Studies, 6*(1), 82-96. https://doi.org/10.21512/jas.v6i1.4458

Maboloc, C. R. (2019). The predatory state and radical politics: The case of the Philippines. *Journal of ASEAN Studies, 7*(2), 161-175. https://doi.org/10.21512/jas.v7i2.6163

Macnamara, J. (2008). Internet media and the public sphere: The 2007 Australian e-electioneering experience. *Media International Australia, 129*(1), 7-19. https://doi.org/10.1177/1329878x0812900103

Mahlouly, D. (2013). Rethinking the public sphere in a digital environment: Similarities between the eighteenth and the twenty-first centuries. *eSharp,* 20. https://www.gla.ac.uk/media/media_279211_en.pdf

Mill, J. S. (2003). *On Liberty*. Binghamton, New York: Vail-Ballou Press.

Norris, C. (2008). Video charts: Algorithmic surveillance. *Criminal Justice Matters, 20*(1), 7-8. https://doi.org/10.1080/09627259508552710

Ong, J. C. and Cabañes J. V. (2018). *Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines*. Leeds, UK: The Newton Tech4Dev Network.

Ong, J. C. and Cabañes J. V. (2019). When disinformation studies meet production studies: Social identities and moral justifications in the political trolling industry. *International Journal of Communication, 13*, 5771-5790. https://ijoc.org/index.php/ijoc/article/view/11417/2879

Patton, M. Q. (2005). Qualitative research. *Encyclopedia of Statistics in Behavioral Science.* https://doi.org/10.1002/0470013192.bsa514

Ramasoota, P. (2016). Online social surveillance and cyber-witch hunting in post-2014 coup Thailand. In C.B. Wungaeo, *et al.* (Eds.), *Globalization and Democracy in Southeast Asia* (pp. 269-288). United Kingdom: Palgrave Macmillan.

Rheingold, H. (2000). *The Virtual Community: Homesteading on the Electronic Frontier*. Cambridge: MIT Press.

Schaffar, W. (2016). New social media and politics in Thailand: The emergence of fascist

vigilante groups on Facebook. *ASEAS – Austrian Journal of South-East Asian Studies, 9*(2), 215-234. https://doi.org/10.14764/10.ASEAS-2016.2-3

Sinpeng, A. (2013). State repression in cyberspace: The case of Thailand. *Asian Politics & Policy, 5*(3), 421-440. https://doi.org/10.1111/aspp.12036

Sombatpoonsiri, J. (2017, July 26). As Thailand restricts internet freedom, cyber activists work to keep an open web. *The Conversation.* https://theconversation.com/as-thailand-restricts-internet-freedom-cyber-activists-work-to-keep-an-open-web-80911

Sombatpoonsiri, J. (2018). Manipulating civic space: Cyber trolling in Thailand and the Philippines. *Giga Focus Asia, 3*, 1-11. https://www.giga-hamburg.de/en/publication/cyber-trolling-in-thailand-and-the-philippines

Thorson, K. (2014). Facing an uncertain reception: Young citizens and political interaction on Facebook. *Information, Communication & Society, 17*(2), 203-216. doi:10.1080/1369118x.2013.862563

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Journal, 13*, 203-218. http://ctlj.colorado.edu/wp-content/uploads/2015/08/Tufekci-final.pdf

Valtysson, B. (2012). Facebook as a digital public sphere: Processes of colonization and emancipation. *tripleC: Communication, Capitalism & Critique, 10*, 77-91. https://doi.org/10.31269/triplec.v10i1.312

Vatsov, D. (2018). Logics of propaganda. *Critique & Humanism: Journal for Human and Social Studies, 49*(1), 71-106. https://hssfoundation.org/wp-content/uploads/2017/04/all-KX-49-print.pdf

Who benefited most from fake news, and other questions, answered in three charts. (2017, 22 December). *VERA Files.* http://verafiles.org/articles/vera-files-yearender-who-benefited-most-fake-news-and-other