SSOAR

Open Access Repository
www.ssoar.info

Mass Surveillance and the Militarization of Cyberspace in Post-Coup Thailand

Laungaramsri, Pinkaew

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
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

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY-NC-ND Lizenz (Namensnennung-Nicht-kommerziell-Keine Bearbeitung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by-nc-nd/3.0/deed.de

Terms of use:
This document is made available under a CC BY-NC-ND Licence (Attribution-Non Comercial-NoDerivatives). For more Information see:
https://creativecommons.org/licenses/by-nc-nd/3.0

gesis
Leibniz-Institut
für Sozialwissenschaften

Mitglied der
Leibniz-Gemeinschaft

Mass Surveillance and the Militarization of Cyberspace in Post-Coup Thailand[1]

Pinkaew Laungaramsri

▸ Pinkaew Laungaramsri. (2016). Mass surveillance and the militarization of cyberspace in post-coup Thailand. *ASEAS – Austrian Journal of South-East Asian Studies*, *9*(2), 195-214.

Post-coup Thailand has witnessed a troubling shift toward censorship, surveillance, and suppression in cyberspace. With cyber security ranking prominently on the military's agenda and the expansion of the military's cyber intervention, the country's online infrastructure has undergone politicization, securitization, and militarization. This paper argues that the militarization of cyberspace in Thailand represents the process in which cyber warfare capabilities have been integrated with other military forces and with support from the masses. This process has been effective through at least three significant mechanisms, including mass surveillance, surveillance by the masses, and normalization of surveillance. Social media have been turned into an absolute digital panopticon. Cyber dystopia, created by the 2014 coup and supported by the masses, has served to sustain a 'state of exception' not only within the territorial borders of the state, but also more importantly, within the virtual space of civil society. Cyber surveillance by the military and the masses has continued to jeopardize the already vulnerable Thai democracy.

Keywords: Cyber Dystopia; Cyber Witch Hunt; Mass Surveillance; Militarization of Cyberspace; Thailand

www.seas.at doi 10.14764/10.ASEAS-2016.2-2

creative commons

INTRODUCTION

On 3 May 2016, a group of activists including myself was summoned to a military barrack in Chiang Mai city for an 'attitude adjustment'[2]. The rationale for the summoning, as the commander of the 33rd Military Circle, the third general, Major General Kosol Prathumchat explained, was that my colleagues and I violated the *National Council for Peace and Order* (NCPO) orders, concretely order number 3/2015 which installed "measures to deal with actions intended to

1 The content of this paper was presented at several conferences and workshops including the Forum on Human Rights and Everyday Governance in Thailand: Past, Present, and Future at Harvard University on 6 March 2015; New Media, Cyber Activism and Social Movement in Asia at Harvard University on 1 April 2015; and Thailand Update Conference at Columbia University on 1 May 2015.

2 'Attitude adjustment' is a technique employed by Thailand's military government to subdue its critics and opponents. Those who are summoned for attitude adjustment might be interrogated for several hours or detained without charge and interrogated in the military facilities. The detention period ranges from one to seven days during which the contact to the outside world is prohibited. At the end of the detention session, the detained will be asked to sign a memorandum of understanding (MoU), a formal agreement between the detained person and the military government, stating that the former will no longer be involved in any political activities and will not leave the country without an official permission by the government.

undermine or destroy peace and national security", by staging a protest at the Thapae Gate of Chiang Mai city on 27 April 2016. In response to this accusation, I argued that the gathering was peaceful and did not involve any activities that would be considered as a threat to national security. I also maintained that the assembly of our small group took place in a public arena where similar activities frequently occurred. However, another high ranking military official who was also there, objected. As he contended, our presence at Thapae Gate might not have posed a problem, but when I posted a photo of the group standing there on Facebook with the caption "Freedom, Freedom, Freedom Now!" – that was definitely a political act that violated the law.

The aim of this paper is to examine the interrelation of the state and social media and their contribution to the creation of *cyber dystopia*[3] in post-coup Thailand. Although social media and computer-mediated communication have been subject to control by the Thai state for almost a decade, cyber security has only recently been identified by the army as a significant part of national security. While the militarization of cyberspace has been incorporated into a part of the army's strategies, various tactics of online and offline surveillance have been deployed to monitor both the data and traffic of Thai citizens on the Internet. In the post-coup era where offline activism has been severely suppressed, the Internet has become a primary platform for communication and digital surveillance by the military which has not only served to monitor online activities and intercept electronic communication, but also provided an effective means to arrest dissidents and anti-military activists. Cyber-crime has recently been identified by the Thai army as one of the most significant non-traditional security threats that requires strict mechanism of control. In defending the necessity of the National Cyber Security Bill, Thai Prime Minister Prayuth Chan-ocha firmly asserted: "If there is a threat to national security – a violation, or someone committing a crime – we need to empower state officials to investigate" (Sim, 2015).

The Thai military's shift toward cyber security is a response to the need to find a new role for the Thai armed forces in the 21st century. While, on the one hand, the military continues to increase its surveillance capability across wider social arenas, on the other hand, cyberspace has been discovered to represent a new platform for political empowerment. Militarization of cyberspace is thus the new mechanism for the military to consolidate its political power. As Pirongrong Rananand (2003) argued, the changing political landscape in Thailand has had a profound impact on the Internet regulatory landscape.

The military's attempt to systematically control the Internet began in 2007, following the 2006 coup, when the military-led Surayud government passed the Com-

3 Dystopia brought by digital technology has been discussed by several scholars such as David Nye (2007), Nancy Baym (2010), and Evgeny Morozov (2011; 2013) in the attempt to counter the idea of cyber-utopianism – the belief that online communication provides freedom and emancipation. According to these scholars, the use of digital technology can also result in the individual's inability to control the changes and impacts brought by this new means of communication. Nye (2007) and Morozov (2011) further posit that the development of the Internet has also led to an increased control of society by the elite and demonstrates how such technology represents a false hope of freedom. Baym (2010), on the other hand, suggests that new media have produced fear among those people who increasingly considered that cyberspace will take away the intimacy of social relationships. Following these scholars, this paper uses the term cyber dystopia to refer to the state in which a fearful and oppressive atmosphere has been generated by digital technology used by the state as its apparatus to control its citizens.

puter Crime Act.[4] Although Internet filtering was first initiated in 2002 by the *Ministry of Information and Communication Technology* (MICT), the 2007 Computer Crime Act was the first step to state legalization of information control on the Internet.[5] This law has created substantial penalties for cyber-crimes and placed criminal liability on any person who allowed unlawful content to be distributed, including lèse-majesté (O'Brien, 2014). Since it came into force, the law has been widely criticized for its violation of freedom of expression on the Internet.

In the aftermath of the 2014 coup, cyberspace in Thailand was brought under tremendous political pressure. As social media were the only remaining arena used by the Thai dissidents to wage protest and engage in online activism against the coup d'état, it also became the most effective sphere that the military government could employ to create their political legitimacy, instigate cyber libels against the opposition, and manipulate civil sentiment. In a country with numerous coups d'état, the recent coup has combined online and offline tactics of suppression, including mass-supported surveillance, in an attempt to secure its authoritarian regime (Sinpeng, 2014).

Apart from implementing several forms of Internet regulations, the junta also created new administrative bodies aiming at more effective monitoring and control of online communication. Crimes related to lèse-majesté, national security, or 'infringing' NCPO's orders would be tried and adjudicated by the military court, which lack appellate and higher courts. Activists and political opponents were targeted and arrested based on their social media activities while academics and journalists were summoned for questionings. The military government is also reportedly laying the political groundwork for a dramatic restructuring of the country's Internet landscape through the *Single Gateway* or the *Great Firewall of Thailand* project – a project to consolidate all gateways into one central government-controlled point to allow for easier monitoring and interception of materials deemed inappropriate.[6] If implemented, the proposed single gateway will not only dramatically cripple the country's digital infrastructure, but might also lead to the instability of Internet connections that can result in an immense economic damage ("Government Warns", 2015).

---

4 The Computer Crime Act was first drafted in 2002 during the Thaksin government. It was, however, revised several times, in 2003, 2005, and 2006, before being enacted in 2006 during the military-appointed Surayud government. According to Sawatree Suksri, in the last revision under the supervision of the military-appointed National Assembly, fundamental clauses were removed from the act, especially those related to the protection of human rights. Serious penalty was also suspended on those Internet providers who distributed illegal contents. At the same time what was considered illegal content was very broadly defined and subsequently resulted in random arrests and charges by government authorities. The Computer Crime Act, especially the 2006 revised version, has been heavily criticized as being a tool to control and suppress people who share different political views from those of the government (Sawatree, 2011).

5 Since the implementation of the act, court orders to block Internet content have increased from two URLs in 2007 to over 74,000 in 2012 (Freedom House, 2014).

6 Section 1.2 of the Cabinet Resolution of 30 June 2015 indicates that the Ministry of Information and Communication Technology must proceed with the "implementation of a single gateway to be used as a device to control inappropriate websites and flow of news and information from overseas through the Internet system" ("Govt 'Gateway'", 2015). The proposed project has prompted widespread outcry among netizens who set up a campaign "Go Against Thai Govt to Use a Single Internet Gateway" on change.org. In December 2015, the campaign, which was launched in October 2015, had already earned 152,886 signatures.

Literature on social media has often emphasized the rise of new media and online social networks as one of the major forces that have contributed to novel practices of popular democracy in the last three decades (Anduiza, Perea, Jensen, & Jorba, 2012; Castells, 2007; Clark, 2012; Van De Donk, Loader, Nixon, & Rucht, 2004). Formerly, traditional political movements gave priority to street protests and direct contestation to power holders. The development of communication technologies, however, has altered the nature and dynamics of social movements by stimulating the diffusion of protest ideas and strategies beyond the limit of physical boundaries and modern nation-states. Such changes have also transformed state-citizen relationships and surveillance practices in the political arena. While a growing body of literature recognizes the rise of 'new' social movements and its impacts on the transformation of the political landscape, little attention has been paid to the manifestation of complex political actions interfacing with different ideologically-based social and political movements, particularly with the formation of counter-movements in the public sphere, and their relation to new media.

The linkage between social media and democracy has been widely acknowledged (Trippi, 2004). Yet, while it is often believed that the advancement of the Internet has contributed to the building of a digital civic infrastructure where new ways to access data and network have increased the distribution of information and the political potential as well as the "electronic fabric of struggle" (Cleaver, 1995)[7] within civil society, it is less recognized that the digital has also significantly reshaped the "art of government" (Foucault, 2010).[8] Among the very few studies on the politics of social media, the work of Morozov (2011) offers a critical scholarly perspective on questions of "cyber-utopianism" or the Internet's "freedom agenda" by directing our attention toward the "dark side" of the Internet. According to Morozov (2011, 2013), the new media not only empower visions of democracy and freedom, but also enable the consolidation of authoritarian regimes as they become used by the state to engage in mass surveillance, political repression, and the spreading of nationalist and extremist propaganda. Morozov argues that there are two delusions propagated by scholars and activists of new media and social movements: The first is "cyber-utopianism" (Morozov, 2011, pp. xiii-xiv), or the belief that Internet culture is inherently emancipatory; and the second is "Internet-centrism" (Morozov, 2011, pp. xv-xvii), or the propensity to view all political and social change through the lens of the Internet. By using a number of cases worldwide to illustrate how the Internet did not eventually deliver the democratizing effects it promised, Morozov points to the dramatic repercussions of the Internet's political role: the appropriation of the online sphere by the authoritarian regime to crack down online activism; the employment of social networks to infiltrate protest groups; or the online seeding of state propaganda in order to more

7 The term was coined by Cleaver (1995) to refer to the use of electronic media in the Zapatista revolution which expanded to computer-mediated communication channels.

8 In the case of Thailand, the rise of social media has stimulated a new form of computer-mediated communication and a rapid flow of information and ideas from various sources – nationally, regionally, and globally. Yet, as Soraj Hongladarom (2000) recently pointed out, online communication in Thailand has been mediated predominantly by 'Thai' culture: Strict prohibition of popular websites and discussion forums, such as Pantip.com, and self-censorship on certain topics, such as those related to the Thai monarchy, are a common moral practice among Thai cyber citizens.

effectively control the movement of the opposition. Contrary to the ideal of political emancipation, Morozov contends that the Internet can in fact contribute to the tightening and suppression of freedom.

Gunitsky (2015) takes the argument of social media effects even further. In authoritarian regimes, he argues, many states have significantly shifted their strategy of social media suppression toward cooptation as another potential mechanism of regime resilience – this is the latest development of authoritarian state-social media relation. Non-democratic regimes are increasingly moving toward pro-actively subverting social media for their own purposes. The objectives are to undermine the opposition, to influence the contour of public discussion, and to gather information regarding "falsified public preferences" (Gunitsky, 2015, p. 42). Tactics such as *counter-mobilization* of supporters and *discourse-framing* of the larger national discourse are used in order to maintain the legitimacy of the regime through social media. Furthermore, regimes can utilize digital technologies to mobilize their own domestic allies, including regular citizens motivated by patriotism, ideology, or other interests (Gunitsky, 2015, p. 45). The antipode of Internet freedom is thus not only Internet censorship but also a combination of control, cooptation, and manipulation. While dimensions of control and suppression have long been acknowledged in scholarly work on the Internet, the aspect of non-democratic regime surveillance has been largely disregarded (Greitens, 2013).

Following a critical view toward social media and the authoritarianism nexus, this paper investigates the role of the Internet in the military regime in post-coup Thailand. Although new media have prompted the growth of online pro-democracy activism among Thai civic groups over the past decades, they have also been increasingly employed to mobilize and establish an absolute royalist ideology. Apart from the military regime's strategies to censor and suppress oppositional political views, social media have also become the arena for a significant counter-movement; this is the right-wing initiative, mobilized to instigate nationalist sentiment and pro-military ideology. Since the 2014 coup d'état, when social movements in Thailand increasingly moved online, the militarization of cyberspace has become an "apparatus of security" where the liberal civic sphere of social media is appropriated and turned into a domain of "governmentality" (Foucault, 2010). Increased control and surveillance by the state have further transformed the Thai political landscape into a 'predator-prey' battleground, while widespread opposition and protest has in turn heightened the military's sense of insecurity and thus surveillance efforts. It is worth noting that over the past five years the nature of the military surveillance system has shifted and intensified in several ways (Sinpeng, 2014). First, cyberspace has become the military's priority battlefield. Second, Internet surveillance has been attached to the military's security agenda and institutionalized within the new military state. Third, the surveillance agenda has been integrated into a variety of administrative institutions, such as in the newly established Army Cyber Center, the Ministry of Information and Communication Technology, the Police Department, and the Ministry of Justice. And fourth, the military's support of popular denunciation has become part of a campaign that serves to perpetuate and expand surveillance in order to eliminate ideological enemies. All of these efforts aim to uncover the so-called network of the anti-monarchy and conspiracies against the regime.This paper argues that the mili-

tarization of cyberspace in Thailand represents the process in which cyber warfare capabilities have been expanded through other military forces and with the notable support from the urban middle-class masses. This process has been effective due to at least three significant mechanisms including mass surveillance, surveillance by the masses, and the normalization of surveillance. While in many countries, cyber militarization has primarily been an outward move toward external security threats, Internet militarization in Thailand, however, has been designed as a specific weapon that turns against internal threats and thus its own people. The 2014 coup and the post-coup government have turned social media into an absolute digital panopticon aimed to thwart protest, to wreck potential networks of dissents, and to infuse public fear. Some scholars call this phenomenon the "cyber coup" (Sinpeng, 2014), while others dub it "the martial law of the online" (Arthit, 2015). I argue that the cyber dystopia created by the 2014 coup and supported by urban middle-class masses has served to sustain a state of exception – the suspension of the rule of law in the name of the public good (Agamben, 2005) not only within the territorial boundaries of the nation, but also within the virtual space of civil society. The collaboration of mass surveillance and surveillance by the masses not only works to jeopardize Thai democracy but also to stifle the culture of individual freedom within Thai society.

MASS SURVEILLANCE

Mass surveillance and secret warrants are not new in Thailand. During the Cold War period, Thailand was the region's largest information-gathering base for the United States and served as the center of intelligence gatherings from different countries over the world (Kavi, 2013). Anti-communist operations were carried out both by the police and the army. Such operations included censorship, spying, purges, and imprisonment of those who were suspected as communist and communist sympathizers. In the post-Cold War era, mass surveillance against communism subsided. The Anti-Communist Act was repealed in 2001 and many intelligence agencies such as the *Internal Security Operation Command* (ISOC) found themselves without mission. Under the Prayuth regime, the expansion of mass surveillance and the emphasis on cyber surveillance has put in place a new form of digital panopticon that differs both in scope and scale from that of the Cold War mission.

From the first day of the declaration of martial law, the military has initiated cyber warfare by systematically controlling the mass and social media.[9] Many junta orders were issued to forbid traditional broadcasts from distorting news reports, to censor online news, and to arrest hundreds of critics (Freedom House, 2015). At the same time, several technologies have been used to block and censor the Internet, such as caching, blacklisting domain names or IP addresses, or redirecting to a government

9 Although cyber warfare is often defined as actions by a nation-state to penetrate another nation's computer-based information system and networks in order to disable or disrupt essential services (Clarke, 2010), the Royal Thai Army uses the term to refer to military operations to eliminate cyber-crimes that posed serious threat to the internal security of the nation. As Major General Kongcheep Tantrawanich, spokesman for the Ministry of Defense, stated, in the past, each branch of the armed forces worked uncoordinatedly in dealing with cyber-attacks – the establishment of a *Cyber Warfare Unit* will enhance the army's ability to work effectively in order to ensure the cyber security of the country ("Cyber Warfare Unit", 2015).

homepage.[10] These measures are apparently employed in order to make 'unsuitable' websites appear unavailable.

Censorship

On 28 May 2014, Facebook was temporarily blocked for around one and a half hours in the afternoon by the MICT in order to silence the anti-coup protest. According to the *Bangkok Post*, up to 30 million accounts across Thailand were affected by the Facebook outage (Achara, 2014). In response to media criticism, the NCPO denied responsibility for the blocking, claiming that the problem was a gateway glitch. However, international media such as Reuters cited Surachai Srisaracam, permanent secretary of the MICT, in an interview stating:

> We have blocked Facebook temporarily and tomorrow we will call a meeting with other social media, like Twitter and Instagram, to ask for cooperation from them . . . . Right now there's a campaign to ask for people to stage protests against the army so we need to ask for cooperation from social media to help us stop the spread of critical messages about the coup. (Petty, 2014)

According to Freedom House (2014) – a US-based human rights advocacy organization – a spokesman for the Telenor Group, owner of the DTAC mobile network operator, told the Norwegian *Aftenposten* newspaper that the telecommunications regulator *National Telecommunication Commission* (NBTC) had ordered mobile networks to block Facebook on 28 May 2014. However, in the wake of this unauthorized remark, an NBTC official warned DTAC for its "inappropriate comment" and threatened to investigate its foreign shareholder percentage and to ban it from the upcoming 4G spectrum auction. As a result, Telenor issued an apology for actions which "damaged the public image of the NBTC and the NCPO" ("DTAC Punished", 2014).

A report from the Citizen Lab (2014) indicates that since seizing power in May 2014, Thailand's military junta has blocked hundreds of websites deemed a threat to national security. In the semi-annual report of the Royal Police Department, Police General Somyos Pumpanmuang, Commissioner General, claimed that in the latter half of 2014 the Police Department closed down 25,069 websites disseminating lèse-majesté content ("Six Months Report", 2015).[11] Freedom House ranked Thailand's Internet freedom in 2014 and 2015 as "Not Free" – a very low status in comparison to its neighboring countries, such as Myanmar which was ranked "Partly Free" in 2014

10 Blacklisting websites is ideal for this kind of web censorship since webmasters are usually unaware when their websites become blocked (Race, 2004).

11 Unlawful contents are usually classified by the police and relevant authorities into seven broad categories including pornography, sale of sex equipment, threats to national security, which includes criticisms of the monarchy, illegal products and services, copyright infringement, illegal gambling, and others. Statistics by the Royal Police Department show that prior to the 2006 military coup, the top illicit websites reported were mostly relating to pornography ("Illicit Website Reported", n.d.). The shift toward lèse-majesté or threats to national security as the prime target of censorship in the period after the 2006 coup reflects an increasingly turbulent political situation in Thailand where the use of lèse-majesté has become a political tool to suppress dissident views against the military government.

(Freedom House, 2014, 2015).[12] Clearly, in the aftermath of the coup, the numbers of websites that became blocked escalated with reasons shifting toward the violation of the lèse-majesté law.

Lèse-majesté law – a criminal code to protect the dignity of the majesty and members of the royal monarch – has an intriguing history. The law dates back to 1908, when the country was under the absolute rule of the monarchy. Since 1932, when democracy was adopted with the King as head of the state, the protection of the King has continued to be recognized in the constitution and specifically in the Criminal Code under the Article 112. Any defamation, insult, or threat to the King, the Queen, the heir-apparent, or the Regent will be punished with imprisonment of 3 to 13 years. However, as some scholars have observed, in the transition to democracy, the use of lèse-majesté in Thailand has been intensified – a tendency opposite to that of other countries with similar constitutional monarchies (Somchai & Streckfuss, 2008). Between 1990 and 2005, only a few lèse-majesté cases per year were recorded and in some years (1993, 2002), there were no new cases received by the prosecution department at all (Streckfuss, 2011, p. 111). But the statistics have increased 15 times between 2006 and 2011, with more than 400 cases being tried, and in most cases, bails were denied. Since the military coup in May 2014, more than 50 lèse-majesté cases were brought to trial, three out of four of which were related to online message posting or sharing. Under the military courts, even harsher sentences were enforced. In August 2015, a tour operator and a hotel worker were sentenced to 60 and 58 years respectively for an article posted on Facebook. The sentences were reduced to half after a guilty plea ("Thai Courts Give", 2015). The incident marks the longest recorded sentence for lèse-majesté in the Thai history.

The intensification of lèse-majesté law over the past decade demonstrates a certain connection between the enforcement of this law and the political instability of Thailand. Censorship and political cleansing has been carried out extensively by several junta governments in order to thwart their opponents and weaken the democratic civil society. The far-reaching use of lèse-majesté law has turned Thailand into what Streckfuss (2011) calls the "defamation regime" where rules of law and freedom of speech have been suspended. As the definitions of insult and defamation have never been clearly explained, and details of the charges are never publicized under the pretext to avoid repeating the offensive remarks, the allegation of lèse-majesté can be random and arbitrary while the accusation can be made against anyone. A self-perpetuating mechanism of surveillance, the law along with other related legislations such as the Computer Crime Act have become the most draconian tools employed by the junta to stifle the right of the people to freedom of expression, both in the real/physical and virtual realms.

Deception/Interception

Deception was a more advanced tactic used to deceive Facebook users in order to gain access to personal information. According to the Thai Netizen Network, a Bangkok-based digital rights group, the Thai police's *Technology Crime Suppression Divi-*

12 Thailand's status of Internet freedom declined after the year 2013 when it was still rated as "Partly Free" (Freedom House, 2014).

sion (TCSD) created a fake Facebook application which was part of the government program to monitor access to blocked websites ("Thai Police Create", 2014). In this application, users were asked to provide personal details such as their date of birth and email address. When users entered the page, four buttons would appear on the webpage – "Close", "Sign in with Facebook", "Sign in with Google", and "Sign in with Microsoft". If users clicked "Close" or "Sign in with Facebook", they would be directed to a Facebook page which then asked the users to grant permission for an application called "Login" to access the users' email addresses and public profiles. If users clicked "Sign in with Google", they would be redirected to a Google page which also asked the users to allow an application called TCSD to access the same kind of information. Through these fake applications, users were under the impression that they were merely logging into a website via Facebook or Google. But by entering their information, users unintentionally gave permission to the TCSD to access personal data stored on their Facebook pages.

The tactic of deception via fake online applications was twice suspended by Facebook. However, Prachatai noted that hundreds of email addresses had already been harvested ("Thai Police Create", 2014). It is not clear how many suspects were arrested specifically because of their activity on social media, yet iLaw reported that by 21 August 2014 there had been 257 arrests for offensive comments; 30% of these (77 cases) were charged due to comments made on the Internet. Additionally, numerous charges concerning the violation of the lèse-majesté law were carried out through the interception of online activities.

To equip the surveillance bureaucracies with greater capacity, the Thai cabinet also approved eight draft bills which were planned to transform the country's economy into a 'digital' economy.[13] Among these bills was the notorious Cyber Security Bill which was designed to restructure and tighten the control of telecommunications in Thailand. If further approved by the National Legislative Assembly, the bill would create a *Cyber Security Commission* – a new body headed by the prime minister and authorized to access any type of digital information from the country's providers of communication services without a court order. With full authority, the commission could also order all public and private organizations to cooperate against any perceived threat to national cyber security, summon individuals for questions, and grant legal power to any appointed officer to access emails, instant messages, and other forms of text-based communication as well as demand access to information on any computer system and listen to any voice conversations on any network in Thailand (Silfversten, 2015). With this bill, the martial law would be normalized and turned into an actual law that would grant the MICT and the new state apparatus unlimited power and the most alarming means of surveillance in the digital history of Thailand.

13 The eight draft bills are parts of the Digital Development Plan for Economy and Society put forward by the *Committee on Preparations for Digital Economy and Society*, chaired by Prime Minister Prayuth Chan-ocha. The plan covers 20 years of an administrative reform in order to establish the digital foundation of the country and to introduce digital technology in all sectors of the country. Eight items of the legislation were proposed to be amended and approved as part of the plan. These include the (1) Electronic Transaction Bill (amendment); (2) Cybersecurity Bill; (3) Computer-Related Crime Bill (amendment); (4) Personal Data Protection Bill; (5) Digital Economy Promotion Bill; (6) Digital Development for Economy and Society Fund Bill; (7) Broadcasting and Telecommunication Regulator Bill (amendment); and (8) Electronic Transaction Development Agency Bill (amendment) (Zeldin, 2016).

SURVEILLANCE BY THE MASSES: CYBER SCOUTS AND CYBER WITCH HUNTS

The militarization of cyberspace has been effective not only through the technique of mass surveillance, which has been deployed in various administrative organizations, but also, importantly, through the establishment of surveillance by the masses. Military support of this process has been both direct and indirect as surveillance by the masses developed in both organized structures and more impromptu forms and settings. Some organized surveillance networks of netizens have been initiated and supported by the government while others act independently. In the aftermath of the coup, the right-wing movement of the *People's Democratic Reform Committee* (PDRC) has transformed into a para-military network of netizens, assisting the military to wage cyberwar against the opposition. Two significant programs that are actively at work are the *Cyber Scout Program* and *Cyber Witch Hunt* organized by the *Garbage Collecting Organization* (GCO).

Cyber Scouts

The Cyber Scout Program was developed in 2010 by the Ministry of Justice and the Ministry of Information and Communications and Technology during the military-backed Abhisit government. It lapsed for several years and re-emerged again after the 2014 coup. The program is currently under the auspices of the MICT. The objective of this program is to create a network that collaborates to eradicate 'unsuitable' and 'disrespectful' websites and to build a network of volunteers to protect the monarchy in the online sphere. Unlike *Village Scouts*[14] in the 1970s, the patrolling power of Cyber Scouts extends beyond the limits of physical boundaries.[15] Currently, there are 112 schools committed to the program which have signed a memorandum of understanding with the MICT. The MICT also claimed that it has so far 'recruited' more than 120,000 Cyber Scouts nation-wide and plans to double the size in the near future.

Cyber Scouts are needed in order to enhance the state's capacity of surveillance. As Farrelly (2010) noted, the past efforts of the government to police the Internet have enjoyed only partial success. Although the military is able to block a number of websites, many of them re-surface with new IP addresses and new cohorts of Internet users. At the same time, contentious content could be copied and redistributed, made more attractive and disseminated more widely. Notably, the reinvention of Cyber Scouts also represents a significant mechanism to indoctrinate young Internet users with ultra-royalist values. This agenda is timely, especially since university stu-

14 Village Scout was a country-wide organization founded by the Thai Border Patrol Police under the aegis of the Ministry of Interior during the 1970s. Sponsored by the King and the Queen of Thailand, the aim of the organization was to promote national unity and to counter the communist insurgency. Organized in small cells and trained in a five-day training course, Village Scouts acted as the surveillance apparatus of the state and would inform local officials about suspicious incidents such as strangers entering the villages. During the short period of the Village Scout establishment, it was estimated that over five million Thais, or 10% of the population had completed the training program prerequisite to becoming a Village Scout (Muecke, 1980, pp. 407-409).

15 Since today's boy-scout program is under the patronage of the King, it was easy to integrate the agenda of cyber surveillance into existing boy-scout activities.

dent movements have become more active in demanding democracy and freedom of expression. The program thus works as a counter-movement to thwart the potential growth of the student movement by turning school students into secret police.

One Cyber Scout interviewed by AFP was a 39-year old school worker in Bangkok who patrolled the Internet pages on his computer in search of offensive remarks that might constitute lèse-majesté (AFP, 2011). Trained in a one-day Cyber Scout camp, this man told AFP: "My inspiration to be a Cyber Scout is the King. There are many ways to protect the institute, and this is one of them" (AFP, 2011). Like other Cyber Scouts, he would roam around certain websites and social networks in his free time and look for seemingly insulting posts. He claimed that he had not reported anybody to the authorities yet. But he assured AFP that if he found any comments deemed offensive to the King, he would immediately contact the person who posted them. "Not many people know about the project. They may think they are talking to a friend because I don't tell them I'm a Cyber Scout", he said (AFP, 2011).

In the post-coup era, cyber vigilantism and the 12 core values of the Thai schools' motto promoted by the Prayuth regime work hand in hand in transforming schools across the nation into a panopticon unit of virtual surveillance to both protect the royal institution and further nurture the ultra-royalist ideology.

Cyber Witch Hunts

Historically, witch hunting, both literal and metaphorical, has always been characterized as an attempt to impose conformity to the ideology of the dominant class (Federici, 2004). The practice of witch hunting involves an investigation of subversive activities in order to harass and punish those people with differing views. This was equally true for the Cold War era in Thailand when the label 'communist' could put one in jail and thus forced many people to join the insurgent movement in the jungle (Thak, 2007). Fear is used to regulate societal behavior while punishment is enforced on the divergent in order to bring conformity and order into society. In the history of anti-communism in Thailand, rumor was enough to bring somebody to trial, usually resulting in the imprisonment of the accused. In many cases, the alleged communists were hunted down and violently killed as suggested by the phrase, coined by people in the south of Thailand: "*Theeb Long Khao Phao Long Thang Dang*", literally meaning "kicking [them] down the mountain, burning [them] in the red tank" (Pornteap, 2012).[16]

Cyber witch hunting in contemporary Thailand centers around accusations of anti-monarchy ideology disseminated online. This ultra-royalist movement acts in various forms, both individually and collectively. Some journalists estimated that there were more than 20 ultra-royalist groups that work to monitor the Internet in order to wipe out any criticism of the monarchy and hunt down offenders (Thouvenot, 2014). Many of the group leaders are associated with the military, some being former military officers or supporters of the coup. One of the most active groups is the Garbage Collecting Organization. This group is led by the Director of the Mon-

16 It was estimated that more than 3,000 people in Southern Thailand were killed during anti-communist purges and witch hunts in the 1960s and 1970s (Pornteap, 2012).

gkut Wattana General Hospital in Bangkok, Major General Rientong Nan-nah. The GCO Facebook page was set up in 2014 with currently more than 242,680 likes. The goal of the organization is to mobilize people to assist in witch hunting and increase the charge against those identified as 'garbage'[17]. GCO also provides online training for those who wish to become professional in hunting down anti-monarchy Internet users. The recent death of the King has witnessed an escalation in witch hunting by ultra-royalists who individually and collectively harassed or threatened those who were accused of being disrespectful to the deceased monarch. Those who did not demonstrate proper mourning etiquette, such as wearing black clothing, could be targeted for bullying, both physically and in virtual spheres (Teeranai, 2016). Online expressions of indifference toward the passing of the monarch were also dangerous as the person who posted such expressions could be hunted down by an angry mob or encounter a violent reaction by the organized royalist group ("Angry Mob Demands", 2016). Most of the incidents of witch hunts took place in the acknowledgement of the government officials.

Witch hunting is often accompanied with the infusion of mass hate. According to Ling (1996), mass hate is a form of social hysteria that emerges in response to a "socially stressful situation", especially in cases of a perceived threat to the moral boundaries of the community. Social stress may develop from shifts in authority or control and from the recognition of a boundary crisis. Advancement of mass hate additionally depends on the existence of groups which can be vilified. Ling (1996) also argues that mass hate is often established by identifying a 'scapegoat' as a powerful adversary, who, if not under control, will pose a threat to society. "Patterned labeling" is then used to identify the 'deviant' and to make the crisis tangible by drawing the boundary between appropriate and inappropriate behavior (Ling, 1996). In many cases, the deviant might also be subject to what Garfinkle (1956) called a "degradation ceremony" – a public act in which the accused is given a derogatory label and is publicly punished or compelled to recognize the moral superiority of the accusers. At the same time, as Ling (1996) argues, the definition of deviance may develop and change as the crisis continues and self-proclaimed "righteous believers" become more proficient in identifying the nuances of deviance.

Online mass hate in Thailand has proliferated, especially in the transitional period of the post-coup era. Cyber-smearing and systematic scapegoating have mushroomed to target people defined as 'Red Shirt', 'Red Shirt supporter', and 'opponent of the military government'. Patterned labeling such as 'anti-monarchy' (*Lom Chao*), 'traitor' (*Khaai Chad*), or other pejorative names have been created and used in degradation ceremonies where members of the pages collectively join in the process of cyber-libel to damage the reputation of an individual or a group.

THE RISE OF THE CYBER RIGHT-WING MOVEMENT

The emergence of the Thai right-wing movement in the post-Cold War period and especially after the 2006 coup is a subject that has gained little systematic investiga-

17 According to Rientong Nan-nah, the term garbage refers to those people who have never realized the royal grace of the King and who have continued to recklessly commit crimes of lèse-majesté. Those people, as Rientong insists, should not be considered human but the garbage of the country ("I Will Fight", 2015).

tion. Nidhi Eeowsriwong (2013), a renowned Thai historian and social critic, is probably the only scholar who attempted to explain the PDRC phenomenon. Lending on Hannah Arendt's (1973) notions of the "masses" and "totalitarianism", he understands contemporary Thai masses (i.e., members of the urban middle classes in Thai society who support the military regime) as the product of the totalitarian regime. Nidhi (2013) understands the mass as the power basis of a totalitarian dictatorship. The mass is neither mobs, nor classes, but consist of atomized individuals. Isolated and having no tie to any political party or social relations, masses are prone to be indoctrinated toward unconditional loyalty to the totalitarian regime. Well-aware of the differences between the WWII Europe and present-day Thailand, Nidhi (2013) argues that a totalitarian-styled political movement is on the rise in Thailand. Similar to the Nazis in interwar Europe, the PDRC's adherents – people who are "free from all attachments that they once had", "unable to think anything aside from competing in the market in order to preserve their lives", finding their lives "bleak, desolate, and meaningless", "abandoned by politicians, by bureaucrats, by the media, by everything that comprises their existence" – yearn to be mobilized as part of the "meaningful" political movement (Nidhi, 2013).[18]

Thai society, Nidhi (2013) argues, is transforming into an atomized and isolated mass-based entity where the members' radical loss of self-interest and indifference has turned their passionate inclination toward the only remaining string of obligation – their superfluous loyalty to the monarchy. Since loyalty to the monarchy is the only social and moral bond between the masses and the nation, the only way to maintain this bond is to 'unfriend' (in the online realm) or to physically get rid of those who do not share the same loyalty.

The online surveillance masses who represent the contemporary right-wing movement, adhere to certain political views, despite their overall distrust in political parties. Believing that social stratification and inequality are natural, normal, or even desirable, the Thai right-wing masses justify their position by referring to the basis of natural law and the claim of the Thai traditional principle of morality (*Khwaamdi*, *Khunnatham*). Although their political views resonate with those of the previous right-wing forces in the 1970s, the components of the 21st century Thai masses are different from those of their predecessors. They are not rural or gangster-like Village Scouts, Red Gaurs[19] or *Nawapon*[20] , organized by the elite classes. On the contrary, these masses consist of educated tech-savvy middle-class urbanites, who are

18 See also an excellent review of Nidhi Eeowsriwong's articles by Tyrell Haberkorn (2014).

19 The Red Gaur or *Krathing Dang* was a right-wing paramilitary organization established by the Internal Security Operations Command of the Thai military to counter the country's student movement after the democratic revolution of October 1973. Members of the group composed of resentful, young, unemployed, vocational school students, and high school drop-outs, while the major cadres were veterans of the Vietnam War, former mercenaries in Laos, and former army soldiers dismissed for disciplinary contraventions (Baker & Pasuk, 2009, p. 192).

20 The *Nawapon* (new force/ninth force) was a right-wing group of militia, police, Buddhist monks, and others, active during Thailand's short democratic period in the mid-1970s. The organization was supported by the Internal Security Operations Command of the Thai military with an aim to counter the people deemed subversive or communist, including students and members of the labor union. Key supporters included Kittiwuttho Bhikkhu, a monk popular among the right-wing who notoriously stated that killing communists was not demeritorious (Baker & Pasuk, 2009, p. 192).

capable to work both independently and collectively. Unlike the Red Shirt movement whose network and decisions to act are tied to the *Pheu Thai Party* (PTP) and directives by the *Bangkok United Front for Democracy Against Dictatorship* (UDD); these right-wing masses are not based on any formal structures. Since they are individuals who are loyal to the only one supreme monarch, they are ready to form coalitions with any group of people who share the same ultra-royalist ideology. The ability to form coalition across classes has more or less contributed to both the success of the PDRC's movement in general (Pitch Pongsawat, 3 April 2015) and the strength of cyber surveillance by the masses in particular. In the post-PDRC movement, these atomized coalitions have transformed themselves into the surveillance mass of cyber witch hunters who have moved their battlefield from Ratchadamnoen Road to cyberspace. With or without the military regime, this right-wing movement will continue to sustain itself and work as a counter-movement against the perceived anti-monarchy network.

NORMALIZATION OF SURVEILLANCE

In the UK, Wood and Webster (2009) used closed-circuit television (CCTV), also known as video surveillance, to demonstrate how, despite its ineffectiveness, this form of modern surveillance has gained popular enthusiasm and demand. The authors identify at least four reasons: First, as a 'security theater' CCTV symbolizes safety in a society where everything is seen to be a potential source of risk, and where fear dominates – as a stage-set form of security, it is a symbol and a performer that deals with risk. Second, CCTV acts in the name of care as much as control. Third, CCTV has become part of the cultural landscape of Britain; members of the society have not only been used for surveillance but have also enjoyed it in a certain way. Fourth, CCTV offers a visual narrative by which watchers are being animated, as if they were watching a TV soap opera – investing feelings and personalizing its contents (Wood & Webster, 2009).

In Thailand, surveillance has become an everyday experience, partly through the military discourse of "returning the happiness [to Thailand]"[21]. Like CCTV in the UK, the Thai junta's Internet surveillance claims to act out of care and with the aim to prevent political risk. Alongside tight media, Internet censorship, and the arrest of political dissidents, the junta government launched the campaign "Returning Happiness to the People" aiming "to create an atmosphere to gain trust and build confidence" ("Thailand Military Leaders", 2014). Happiness, as claimed by Prime Minister

21 "Returning Happiness to Thailand" is a song promoted by the Thai military right after the 2014 coup. The lyrics were written by the junta leader and Prime Minister Prayuth Chan-ocha which features lines such as "we offer to guard and protect you with our hearts" and "we are asking for a little more time" (Campbell, 2014). The discourse of "Returning Happiness to Thailand/Thai People" was subsequently turned into a military campaign and a Friday night show where the Thai prime minister appears on all free TV channels to address the nation and to provide updates about the work of the government. The Friday night show would usually run for an hour or longer in the time slot generally reserved for the soap operas. In response to the public complaint about the length of his weekly address at the prime time of the TV program, Prayuth stated that: "I talk on Fridays for you to listen and not just watch lakorns [soap operas]! I'll put up loudspeakers and broadcast into every village! Don't be bored by me – no PM has ever done such thing before!" (Saksith, 2015).

Prayuth, had long since gone from Thailand: "The Thai people, like me, have probably not been happy for nine years" (Hodal, 2014). In the months following the 2014 coup and amidst military threats in various media, including social media, a song titled "Returning Happiness" was written by Prayuth himself, free concerts with female dancers dressed in revealing military fatigues were organized, public petting of horses was provided by the army's mounted guard, and Prayuth's weekly TV show, in which he sometimes speaks for more than an hour, was aired every Friday night.

As Wood and Webster (2009) recognize, surveillance works at the level of emotions, symbols, and culture. The normalization of surveillance becomes consolidated when surveillance colonizes these domains. Thus, it is not only the proliferation of surveillance technologies that makes surveillance an everyday experience, but also the way in which surveillance operations are embedded in the norms and institutions of society. In justifying the military's takeover of the country and its subsequent draconian surveillance scheme, Prayuth cited the loss of the Thai value of morality, which he claimed had been destroyed by politicians and prolonged political divisions: "People started to lose trust and faith in the whole system . . . laws were not being respected. We were thus becoming an immoral society". This was the central reason to stage the coup and put the country back in 'order':

> A society without morality, without virtue, without good governance, could not move forward, . . . we were unhappy, so I had to ask myself, 'Can we let this continue?' . . . So, what we are doing today is to try and bring everything back to normal. We intend to return happiness to everyone. ("Thai Police Threaten", 2014)

CONCLUDING THOUGHTS ON CYBER DYSTOPIA

Over the past two years since the 2014 coup d'état, mass surveillance in the name of 'happiness' has become a 'normal' part of everyday life, while the violation of human rights has become an anticipated form of governmentality by the urban masses. In response to media criticism, Prayuth confidently stated: "The coup d'état did not cause any trouble to people, except to those who lost their political power. Same with the draft of the Digital Bill . . . . What do you have to fear about if you have done nothing wrong?" (Royal Thai Government, 2015). The domestication of surveillance has not only brought surveillance closer to homes, but has also integrated it as part and parcel of 'good virtue'. Surveillance, as Prayuth's statement implies, creates "security" and "happiness", and not fear, for people of "good virtue" in Thailand.

The militarization of cyberspace through mass surveillance and surveillance by the masses, normalized by the everyday speech of "happiness" and the need to ensure a smooth transition of Thai society propagated by the military, continues to characterize contemporary Thailand. In a country where fear has been produced, manufactured, and woven into the discourse of security and morality, freedom of speech and expression has been cast out as 'un-Thai' and 'disloyal' to the nation. But as the line that separates right from wrong has never been clear but arbitrary, machinations of fear have become a flourishing industry which can be used by anyone to threaten political opposition. Furthermore, the definition of loyalty has now been extended

beyond the traditional sphere of monarchy-citizen relationships. A recent arrest of a man who shared a video alleged to mock and defame junta leader Prayuth Chan-ocha (Pravit, 2016) suggests that Thai authoritarianism has been fortified and made untouchable by the tools and power of cyber technology. Cyber dystopia – a world in which the production of fear has been normalized, paternalized, and essentialized through the reification of the threat of violence and abjection – has become an everyday reality for Thai netizens (Linke & Smith, 2009). To avoid becoming a victim of such politics of fear, many people have no choice but to stay silent or inactive in order to live safely in the hegemonic totalitarian society.

Militarization of cyberspace in the post-coup era, as I have attempted to show, has not only created a geography of fear based on systematic inclusion and exclusion of particular groups of population, it has also created a desirable type of 'docile population' that could be seduced into obedience by the state's illusory promise of peace and happiness. The creation of new modes of surveillance organization and the expansion of the military ideology of surveillance into the civic realm have led to a redefinition of the concept of security. Cyber dystopia, in the form of a digital panopticon, and cyber cleansing have come to characterize the everyday 'security' of the Thai society.

~

REFERENCES

Achara Ashayagachat. (2014, May 28). Facebook temporarily down. *Bangkok Post*. Retrieved from http://www.bangkokpost.com/print/412255/

AFP. (2011). Thai 'Cyber Scouts' patrol web for royal insults [video]. Retrieved from https://www.youtube.com/watch?v=HAJeSS8-LXc

Agamben, G. (2005). *State of exception* (K. Attell, Trans.). Chicago: University of Chicago Press.

Anduiza, E., Perea, E. A., Jensen, M. J., & Jorba, L. (Eds.). (2012). *Digital media and political engagement worldwide: A comparative study*. Cambridge: Cambridge University Press.

Angry mob demands arrest of man allegedly posting lèse majesté message. (2016, October 15). *Prachatai English*. Retrieved from http://www.prachatai.org/english/node/6654

Arendt, H. (1973). *The origins of totalitarianism* (3rd ed.). New York: Harcourt, Brace & World.

Arthit Suriyawongkul. (2015, January 30). Net citizens said, digital law is the transformation of security law. *Prachatai*. Retrieved from http://prachatai.org/journal/2015/01/57668

Baker, C., & Pasuk Phongpaichit. (2009). *A history of Thailand*. Cambridge: Cambridge University Press.

Baym, N. K. (2010). *Personal connections in the digital age*. Cambridge: Polity.

Campbell, C. (2014, June 10). The Thai junta's 'Happiness' song is a hit! (But who'd dare say otherwise?). *Time*. Retrieved from http://time.com/2851467/thai-coup-junta-happiness-song/

Castells, M. (2007). Communication, power and counter-power in the network society. *International Journal of Communication, 1*, 238-266.

Clark, E. (2012). *Social media & social movements: A qualitative study of Occupy Wall Street*. Huddinge: Södertörn University.

Cleaver, H. (1995) The Zapatistas and the electronic fabric of struggle. Retrieved from https://la.utexas.edu/users/hcleaver/zaps.html

Cyber warfare unit to counter hackers under preparation. (2015, October 23). *Thai PBS*. Retrieved from http://englishnews.thaipbs.or.th/cyber-warfare-unit-to-counter-hackers-under-preparation

DTAC punished for revealing junta's role in Facebook shutdown. (2014, June 11). *Khaosod English*. Retrieved from http://www.khaosodenglish.com/politics/2014/06/11/1402471813/

Farrelly, N. (2010). From Village Scouts to Cyber Scouts. Retrieved from http://asiapacific.anu.edu.au/newmandala/2010/07/02/from-village-scouts-to-cyber-scouts/

Federici, S. (2004). *Caliban and the witch: Women, the body and primitive accumulation*. New York: Autonomedia.

Foucault, M. (2010). *The government of self and others: Lectures at the Collège de France 1982-1983* (F. Gros, Ed.; G. Burchell, Trans.). Basingstoke: Palgrave Macmillan.

Freedom House. (2014) Freedom on the Net 2014: Thailand. Retrieved from https://freedomhouse.org/report/freedom-net/2014/thailand

Freedom House. (2015) Freedom on the Net 2015: Thailand. Retrieved from https://freedomhouse.org/report/freedom-net/2015/thailand

Garfinkle, H. (1956). Conditions of successful degradation ceremonies. *American Journal of Sociology, 61*(5), 420-424.

Government warns netizen protesters. (2015, October 2). *Bangkok Post*. Retrieved from http://www.bangkokpost.com/tech/local-news/714964/government-warns-netizen-protesters

Govt 'Gateway' denials contradict cabinet resolutions. (2015, October 2). *Khaosod English*. Retrieved from http://www.khaosodenglish.com/politics/2015/10/02/1443777645/

Greitens, S. C. (2013). Authoritarianism online: What can we learn from Internet data in nondemocracies? *PS: Political Science and Politics, 46*(2), 262-270.

Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics, 13*(1), 42-54.

Haberkorn, T. (2014). Hannah Arendt, Nidhi Eoseewong, and the spectre of totalitarianism in Thailand. *The Asia-Pacific Journal, 12*(14). Retrieved from http://www.japanfocus.org/-Jeff-Kingston/4105/article.html#sthash.dvgFlEGW.dpuf

Hodal, K. (2014, June 4). Thai junta 'brings happiness to the people' with parties and selfies. *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/jun/04/thailand-to-bring-happiness-to-the-people

I will fight for the King: An interview with Riengton Nan-nah. (2014, April 21). *Post Today*. Retrieved from http://www.posttoday.com/analysis/interview/290242

Illicit website reported since April 2002. (n.d.). Retrieved from http://web.archive.org/web/20060220123137/http://cyber.police.go.th/reporting/report/sum.php

Kavi Chongkittavorn. (2013). Spy me, spy you, sa-bai Thailand. *The Nation*. Retrieved from http://www.nationmultimedia.com/opinion/Spy-me-spy-you-sa-bai-Thailand-30218613.html

Ling, R. (1996). Cyber McCarthyism: Witch hunts in the living room. *Electronic Journal of Sociology, 2*(1). Retrieved from http://socserv2.socsci.mcmaster.ca/EJS/vol002.001/Ling.Article.1996.html

Linke, U., & Smith, D. T. (Eds). (2009). *Culture of fear: A critical reader*. London: Pluto Press.

Morozov, E. (2011). *The net delusion: The dark side of Internet freedom*. New York: PublicAffairs.

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. New York: PublicAffairs.

Muecke, M. (1980). The Village Scouts of Thailand. *Asian Survey, 20*(4), 407-427.

Nidhi Eeowsriwong. (2013, December 31). The great mass of the people (T. Haberkorn, Trans.). *Prachatai English*. Retrieved from http://www.prachatai.com/english/node/3802

Nye, D. E. (2007). *Technology matters: Questions to live with*. Cambridge: The MIT Press.

O'Brien, D. (2014, June 12). Thailand's junta flexes its muscles online. Retrieved from https://www.eff.org/deeplinks/2014/06/thailands-junta-flexes-its-muscles-online

Petty, M. (2014, May 28). Thai ministry sparks alarm with brief block of Facebook. *Reuters*. Re-trieved from http://in.reuters.com/article/thailand-politics-facebook-idINKBN0E80U520140528

Pirongrong Rananand. (2003). Internet and democracy in Thailand. In I. Banerjee (Ed.), *Rhetoric and reality: The internet challenge for democracy in Asia* (pp. 288-317). Singapore: Eastern University Press.

Pornteap TT. (2012, February 3). Kicking down the mountain, burning in the red tank: The polarization of ideologies and witch hunts in Pattalung Province [blog entry]. Retrieved from http://pornteap.blogspot.co.at/2012/02/blog-post_03.html

Pravit Rojanaphruk. (2016, February 1). Libel unclear in 'illegal' video mocking Prayuth. *Khaosod English*. Retrieved from http://www.khaosodenglish.com/politics/2016/02/01/1454320405/

Race, J. (2004). Censoring the Internet in Thailand. Retrieved from http://www.camblab.com/nugget/block/block_01.htm

Royal Thai Government. (2015, September 9). Returning happiness to Thai people. Retrieved from http://www.thaigov.go.th/index.php/th/program1/item/106682-id-106682

Saksith Saiyasombat. (2015, June 1). Infographic: Thai junta leader to cut short 'boring' Friday night rants. *Asia Correspondent*. Retrieved from https://asiancorrespondent.com/2015/06/infographic-thai-military-junta-leaders-weekly-tv-address-to-reduce-air-time/

Sawatree Suksri. (2011). An analysis of the draft computer crime bill [in Thai]. Retrieved from http://mycomputerlaw.in.th/wp-content/uploads/2011/09/new-cca-analysis-sawatree-201109.pdf

Silfversten, E. (2015). Thailand's Cybersecurity Bill and Internet censorship. Retrieved from http://erik.silfversten.se/thailand-cybersecurity-bill-internet-censorship/

Sinpeng, A. (2014, September 23). The cyber coup. In F. Aulino, E. Elinoff, C. Sopranzetti, & B. Tausig (Eds.), *The wheel of crisis in Thailand. Hot Spots, Cultural Anthropology Website*. Retrieved from https://culanth.org/fieldsights/568-the-cyber-coup

Sim, S. (2015, January 29). Thailand internet censorship: Junta defends cybersecurity laws, or-ders press freedom briefing canceled. *International Business Times*. Retrieved from http://www.ibtimes.com/thailand-internet-censorship-junta-defends-cybersecurity-laws-orders-press-freedom-1799018

Six months report of the police department. (2015, April 25). *Prachatai*. Retrieved from http://prachatai.com/journal/2015/04/58968

Somchai Preechasilapakul, & Streckfuss, D. (2008). Ramification and re-sacralization of the lèse majesté law in Thailand. Paper presented at the 10th International Conference on Thai Studies, 9-11 January, The Thai Khadi Research Institute/Thammasat University, Bangkok, Thailand.

Soraj Hongladarom. (2000). Negotiating the global and the local: How Thai culture co-opts the Internet. *First Monday, 5*(8-7). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/782/691

Streckfuss, D. (2011). *Truth on trial in Thailand: Defamation, treason, and lèse-majesté*. London: Routledge.

Teeranai Charuvastra. (2016, October 16). Ultra-Royalists guilt-shame people who don't wear mourning black. *Khaosod English*. Retrieved from http://www.khaosodenglish.com/politics/2016/10/16/ultra-royalists-guilt-shame-people-dont-wear-mourning-black/

Thai courts give record jail terms for insulting King. (2015, August 7). *BBC*. Retrieved from http://www.bbc.com/news/world-asia-33819814

Thai police create fake FB app to get Thai net users' information, target users trying to open blocked sites. (2014, June 20). *Prachatai English*. Retrieved from http://www.prachatai.com/english/node/4140

Thai police threaten junta's online critics. (2014, June 7). *Japan Times*. Retrieved from http://www.japantimes.co.jp/news/2014/06/07/asia-pacific/politics-diplomacy-asia-pacific/thai-police-threaten-juntas-online-critics/#

Thailand military leaders launch happiness campaign. (2014, June 8). *The Associated Press*. Retrieved from http://www.cbc.ca/news/world/thailand-military-leaders-launch-happiness-campaign-1.2668950

Thak Chaloemtiarana. (2007). *Thailand: The politics of despotic paternalism*. Chiang Mai: Silkworm Books.

The Citizen Lab. (2014). Information controls during Thailand's 2014 coup. Retrieved from https://citizenlab.org/wp-content/uploads/2015/03/Information-controls-during-Thailand%E2%80%99s-2014-Coup.pdf

Thouvenot, D. (2014, June 15). Thai cyber police step up royal slur patrols. Retrieved from http://phys.org/news/2014-06-thai-cyber-police-royal-slur.html

Trippi, J. (2004). *The revolution will not be televised: Democracy, the Internet, and the overthrow of everything*. New York: HarperCollins.

Van De Donk, W., Loader, B. D., Nixon, P. G., & Rucht, D. (Eds.). (2004). *Cyberprotest: New media, citizens and social movements*. London: Routledge.

Wood, D. M., & Webster, E. (2009). Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research, 5*(2), 259-273.

Zeldin, W. (2016, June 14). Thailand: Digital Ministry established as part of National Digital Economy Plan. Retrieved from http://www.loc.gov/law/foreign-news/article/thailand-digital-ministry-established-as-part-of-national-digital-economy-plan/

ABOUT THE AUTHOR

Pinkaew Laungaramsri is Associate Professor of Anthropology at the Department of Sociology and Anthropology, Faculty of Social Science, Chiang Mai University.

▸ Contact: pinkaewl@yahoo.com

ACKNOWLEDGEMENTS

I would like to thank Michael Herzfeld, Duncan McCargo, Pitch Pongsawat, Apiwat Ratanawaraha, Pandit Chanrojanakit, Aranya Siriphon, Tyrell Haberkorn, and two anonymous referees of ASEAS for their constructive comments to improve this paper.