SHAPE SEA

Exploring the Nexus Between Technologies and Human Rights

Opportunities and Challenges in Southeast Asia

Edited by

Khoo Ying Hooi
Deasy Simandjuntak

CHAPTER 2

Digital Rights in Southeast Asia: Conceptual Framework and Movement Building

Tan Jun-E

Abstract

This chapter builds a conceptual framework for digital rights by drawing from digital rights advocates in Southeast Asia, and provides a snapshot of the digital rights movement in the region through the advocates' areas of work, challenges faced, and recommendations for advancing the movement. The conceptual framework proposes four spheres of digital rights, as follows: 1) conventional rights translated to digital spaces, 2) data-centred rights, 3) rights to access to digital spaces and services, and 4) rights to participate in the governance of the digital or the Internet. Empirical observation of the digital rights movement in Southeast Asia reveals that most work has been done on conventional rights translated to digital spaces. The lack of technical capacity is a major gap in addressing digital rights violations that require a deeper understanding of how the technology functions.

Introduction

With sixty percent of its population online[1] and many more getting connected every year, Southeast Asia has stepped into the digital era. Communication is revolutionised with the shrinking of time and space constraints, bringing benefits such as economic empowerment and access to knowledge at an unprecedented level. Yet, as the region reaps these developmental benefits (admittedly, at an uneven rate), the darker side of the digital world also manifests in the form of new authoritarian controls and corporate interests which are little understood by most of the people using the new technologies. Digitally transmitted misinformation is rife, and marginalised communities are targeted by cyber attacks and hateful speech. Civil society celebrates new capabilities and forms of organising afforded by the technology but is taken aback at the speed in which human rights violations are facilitated by the new platforms.

In general, civic space in Southeast Asia is limited and has been observed as narrowing (Gilbert, & Benedict, 2018). Governments in the region have kept a tight grip on its citizens, using mechanisms such as draconian laws to restrict civil freedoms. This

[1] Source: Internet World Stats (2019). See Table 6 for more details.

situation continues into the digital era, where legal frameworks have been updated to cover communication on the Internet, such as anti-misinformation or cyber libel laws which have mushroomed within the region, to enable individual countries to tighten control on online speech. To further illustrate the point, none of the eight Southeast Asian countries assessed under Freedom House's *Freedom on the Net* report in 2018 obtained a "Free" status in terms of Internet freedom. Five Southeast Asian countries gained a "Partly Free" status (Cambodia, Indonesia, Malaysia, Philippines, and Singapore) while three countries were "Not Free" (Myanmar, Thailand, and Vietnam). As stated by the report, not only legal frameworks are employed - other mechanisms include the blocking of content and platforms, manipulating online discussions through astroturfing, and conducting technical attacks against human rights defenders.

To understand the bigger picture of how to defend and uphold rights in this digital age, a good place to start is to observe the frontliners who are already doing it. The first hurdle that we encounter in this endeavour, however, is the lack of understanding or conceptual clarity of what digital rights actually is (Dheere, 2017). This lack of clarity undermines any academic work building upon the concept, to be akin to blind men describing an elephant by touching different parts of its body. Therefore, the first objective of this chapter is to build a conceptual framework of what digital rights is, by drawing from insights provided by digital rights advocates themselves. After forming a clearer picture of digital rights, the second research objective is to look at the digital rights movement in Southeast Asia, specifically the work that advocates do and the challenges that they face in mainstreaming problems of digital rights issues to the rest of civil society and the wider public. As little has been written on this nascent topic in the context of Southeast Asia, this study provides a baseline understanding of where the digital rights movement is at the moment, focusing on gaps to be bridged, thus providing the basis for strategising further in advocacy work.

Data collection was done through focus group discussions with digital rights advocates, at the national levels of Malaysia, Thailand, and the Philippines, and also at the regional level. From the analysis of the data, it was found that digital rights is seen differently according to how "digital" is interpreted and if one approaches it from developmental angles of access and governance. The umbrella of digital rights therefore contains four spheres: 1) through viewing the digital as a space/spaces and thus digital rights as a translation of conventional rights to digital spaces, 2) through viewing the digital as data representation of physical entities, therefore focusing digital rights on data security and privacy, 3) access to digital spaces and meaningful participation, and 4) participation in the governance of the digital or the Internet. Currently, the lack of conceptual understanding of digital rights slows the growth of the movement and weakens the ability of advocates to work together or to communicate the importance of their work to a wider audience. A major gap found is the lack of technical capacity in the digital rights movement, and most of the work on the ground is focused on translating conventional rights to digital spaces.

In terms of theoretical contribution, this chapter contributes to theory building through untangling and abstracting distinct viewpoints that form the complex substance of digital rights, each coming with their body of existing work, historical context, and underlying assumptions. There is a widespread perception in the global digital rights community that Western countries are the subject of most digital rights research, and that research areas most compatible to Internet policy concerns of Western governments and corporations receive more funding and research attention (Remensperger, Schwartz-Henderson, & Cendic, 2018). It has also been pointed out that digital rights is differently perceived and defined in non-Western countries, so much so that local societies may resist the agendas of international digital rights organisations, which are mostly based in the West (Daskal, 2018). This chapter, drawing from perspectives of digital rights advocates in Southeast Asia, fills an important void in academic literature, and channels homegrown insights back into advocacy work in the region.

This study employs qualitative methodology, engaging digital rights and advocates from Southeast Asia in focus group discussions (FGDs) and interviews. A total of five focus groups were conducted: one for regional activists, one each for country-level activists in the Philippines and Thailand, and two for Malaysia2. One supplementary interview was held with a respondent with a regional perspective. The countries were chosen based on two factors: the level of activity in digital rights work and the ease of gaining access to the field, as most of the researcher's contacts of digital rights advocates were based in these three countries. Only three countries were chosen to represent national perspectives in Southeast Asia due to resource limitations in conducting fieldwork. As displayed in Table 1, there was a total of 24 respondents. Data collection was performed in July 2019 in Manila, Kuala Lumpur, and Bangkok. The focus groups were facilitated by the researcher and audio-recorded. Respondents were informed of their rights as research subjects through an informed consent form.

Table 1: Details of Data Collection

Data collection sessions	Location	No. of Respondents
Regional focus group	Manila	5
Philippine focus group	Manila	7
Malaysian focus group #1	Kuala Lumpur	2
Malaysian focus group #2	Kuala Lumpur	4
Thai focus group	Bangkok	5
Supplementary interviews	Bangkok	1 (regional)
Total number of respondents		24

[2] A second focus group was held to accommodate those who cancelled for the first.

The sessions lasted an average of three hours, with the time length varying based on the number of participants. The questions can be divided into two main sections: digital rights (definition and digital rights issues in the region/country), and the digital rights movement (areas of work, challenges, strategies, and recommendations). In the first section, because of the broad nature of the questions, discussions were structured using a workshop style letting the participants express their opinions on post-it notes, clustering the post-its according to theme, and finally using them as discussion points. The second section was conducted in the style of a conventional FGD.

What is Digital Rights?

Digital Rights in the Literature

What is "digital rights"? While "digital rights" has been used in the context of digital rights management, i.e., in managing intellectual property of digital content (e.g., Van Tassel, 2016), this is not what this paper is interested in. Instead, we are looking at digital rights in the context of rights advocacy in the digital era. While the term has been used in academic papers and in practice, the definition of the concept is elusive, as this review has only been able to find one comprehensive definition of digital rights. In a paper that details a process of mapping the legal landscape for human rights online, Dheere provides a working definition of digital rights, with the goal of establishing a reference point of whether a law can be considered to affect digital rights or not:

> *"Digital rights" describe human rights – established by the Universal Declaration of Human Rights, UN resolutions, international conventions, regional charters, domestic law, and human rights case law – as they are invoked in digitally networked spaces. Those spaces may be physically constructed, as in the creation of infrastructure, protocols and devices. Or they may be virtually constructed, as in the creation of online identities and communities and other forms of expression, as well as the agency exercised over that expression, for example, management of personally identifiable data, pseudonymity, anonymity and encryption. Such spaces include but are not necessarily limited to the internet and mobile networks and related devices and practices.* (2017, p.12)

Dheere emphasises that this definition is a work in progress, and no other definition has been found so far. This should not be an indication of the lack of interest in the term or that it is seldom used – indeed, digital rights has been used widely as a term for advocacy, but rarely defined by the actors who use it, as observed by Dheere. It has been argued that digital rights has not emerged as an academic field of its own, because most academic writing on it is not anchored in strong theoretical frameworks, but drawn mainly from empirical observations: on the opportunities and threats to established human rights standards brought about by ICT, on case studies of digital activism, and on norm-setting for human rights protections in the online space (Joergensen & Marzouki, 2015, cf. Dheere, 2017).

As the area of digital rights remains nebulous, some studies on the topic anchor their work on existing frameworks or guidelines instead, mostly in the form of Internet/digital bills of rights or charters, which provide sets of norms and principles agreed upon by various constituencies through stakeholder consultations (Gill, Redeker, & Gasser, 2015; Dheere, 2017; Daskal, 2018; Redeker, Gill, & Gasser, 2018). For example, the *Charter of Human Rights and Principles for the Internet* by the Internet Rights & Principles Coalition (IRPC) outlines ten general Internet rights and principles and provides a breakdown of these rights in 21 articles, using the Universal Declaration of Human Rights (UDHR) as a framework (Internet Rights & Principles Coalition, 2018). Another framework that is oft-mentioned is the *APC Internet Rights Charter* by the Association of Progressive Communication (APC), which organises 31 rights by seven themes.[3] There are many such charters and attempts to create "magna cartas" of sorts of Internet rights. In a comparative study of principles for governing the Internet, UNESCO (2015) identified more than 50 Internet-specific declarations and frameworks. In another attempt on analysing "digital constitutionalism" or initiatives that "seek to articulate a set of political rights, governance norms, and limitations on the exercise of power on the Internet", Gill et al. (2015) identified 30 such initiatives and collected a list of 42 rights which they categorised into seven themes4.

Gill et al. (2015) found that freedom of expression, privacy rights, and the right of access to the Internet were the three most featured out of the 30 digital constitutions studied (27, 26, and 24 times out of 30). Freedom of information, as well as transparency, and openness (of Internet governance processes and of networks), were other focal points which were covered by more than two thirds of the documents analysed (22 times out of 30). Indeed, some studies or documents have found it expedient to narrow down their scope to the top two to three rights and to move along with their analytical work or practical advocacy (Daskal, 2018; Global Network Initiative, 2017; Hope, 2011; Kumar, Prasad & Maréchal, 2017). This may be sufficient if the purpose of the authors is to look specifically at freedom of expression and privacy rights, however, most discussions do identify these choices as main or representative foci of digital rights or human rights in the online space. The challenge then seems to be the lack of a theoretical or conceptual framework to define the boundaries of digital rights, compelling researchers and advocates to choose the rights that are most representative and forgoing some other rights that are deemed less central.

The concepts of digital rights and Internet freedom have been operationalised for the purposes of ranking corporations and countries on their performance of upholding rights in the digital or online space. The Corporate Accountability Index, produced yearly by Ranking Digital Rights, for example, ranks a selection of the most influential Internet,

[3] Accessible at https://www.apc.org/sites/default/files/APC_charter_EN_0_1_2.pdf

[4] 1) Basic or fundamental rights and freedoms, 2) General limits on state power, 3) Internet governance and civic participation, 4) Privacy rights and surveillance, 5) Access and education, 6) Openness and stability of networks, 7) Economic rights and responsibilities.

mobile, and telecommunications companies on their policies and practices that affect their users' freedom of expression and privacy.5 The *Freedom on the Net* report, produced by Freedom House, is also an annual report which produces country reports and ratings on Internet and digital media freedom based on three categories: 1) obstacles to access, 2) limits on content, and 3) violations on user rights6. These reports provide a useful, up to date, and comparative understanding of the global digital rights situation. While the operationalisation of the concepts in these reports does help in concretising the concepts, they focus on the measurement of a list of indicators and do not dive deep into the conceptualisation beyond what is needed for practical application. At the time of writing, Ranking Digital Rights is refining its methodology to include human rights harm in targeted advertising and artificial intelligence, which provides an indication of where digital rights violations are heading towards, but does not situate them within a systemic, big picture framework of digital rights. From the literature review, it is clear that there is much interest in the field of digital rights, however, its development is hindered by the lack of a strong theoretical framework. The next two sections attempt to address this gap.

Building a Conceptual Framework

During the FGDs, digital rights activists and advocates were asked what "digital rights" meant to them and what would be important to include in a definition of digital rights. They were instructed to write down their thoughts on pieces of paper, and then to stick the notes onto the wall. A discussion was facilitated with the group based on the notes posted. In all focus groups, the notes exhibited a similar pattern of two types of notes: overarching statements and specific rights and issues that the participants thought should be included as part of digital rights. Table 2 provides a representative sample of these notes[7] from all the focus groups.

[5] More information can be found here: https://rankingdigitalrights.org/index2019/report/index-methodology/

[6] The report can be found at https://freedomhouse.org/report/freedom-net-methodology

[7] Notes with the same meaning have been omitted.

Table 2: What is Digital Rights? Overarching Statements and Specific Rights and Issues Collected from Focus Group Discussions

A. Overarching statements	B. Specific rights and issues
1. Human rights as it is effected in digital space and technologies	B1 Access to government and other services online
2. Ensure human rights online are same as offline	B2 Access to information
	B3 Access the Internet
3. Civil, human, labour, consumer rights in the digital environment	B4 Access to hardware/software
	B5 Right to assemble
4. Digital rights are human rights	B6 Freedom of expression online
5. Basic principles protecting representational entities in digital spaces	B7 Privacy and data security
	B8 Control and ownership over personal and organisational information
6. Protecting the analogue by protecting the digital	B9 Consumer rights added to digital devices
7. My rights (currently given and fighting for) being reorganised on the Internet and other ICTs	B10 Robust copy left/right understanding, and more access to porn
	B11 Right to seek joy and pleasure
	B12 Right to be consulted on policy issues
8. Based on the Internet Rights & Principles Coalition, Philippine Declaration on Internet Rights and Principles	B13 Informed consent on participation
	B14 Safety to participate
	B15 Right to exist free from violence
	B16 Digital governance
9. Rights that protect against violations of freedoms upheld	B17 Right not to be discriminated
	B18 Right to information (fair use)
10. Rights by design	B19 Access for all
	B20 Right to understand, know, access, create, control the digital (environment, infrastructure, things)
	B21 Privacy from the onset
	B22 Right to publish without interference or fear of reprisal
	B23 Right against hateful speech, harassment
	B24 The right to know how our data is used
	B25 Data flow
	B26 Digital inclusion
	B27 Data protection
	B28 Freedom from surveillance

From discussions on the overarching statements, some observations arose, forming the initial thoughts on the conceptual framework. A key point that stood out is that the distinction between "digital" and "online" was not always clear. Two pairs of polar opposites were often mentioned: online versus offline, and digital versus analogue. In some groups not much distinction was made between the first pair and the second pair, conflating online with digital, implying offline as analogue. However, some groups did unpack these concepts, with the participants emphasising that digital and online are distinct. For example, a respondent stressed that a key card or a facial recognition system to permit access to an office may not be "online" or connected to the wider Internet, however, these are digital devices that make use of digital technologies and therefore are still considered as "digital". It is worth mentioning that the conceptual fuzziness between online and digital is present also in academic literature. The terms of digital rights and Internet freedom, for example, have often been used interchangeably to refer to the same thing8.

The nuance between "online" and "digital" points at two different views of what "digital" means, forking the discussions on the topic into two directions. The first is to view the digital and online as spaces which stand separate from spaces that are analogue, or offline (e.g., "human rights as it is effected in digital spaces and technologies" (A1), "ensure human rights online are same as offline" (A2), and "civil, human, labour, consumer rights in the digital environment" (A3)). In this viewpoint, the translation of existing human rights into these spaces is the basis of digital rights – one respondent claimed that there are no new rights, only a different application and interpretation of existing rights into digital spaces.

The second viewpoint sees the digital as a data representation of physical entities. A definition provided by another respondent, drawing from his organisation's understanding of digital rights, was that digital rights are "basic principles protecting representational entities in digital spaces" (A5). In this view, digital rights infringements on individuals happen when their data is mistreated, hence, one "protects the analogue by protecting the digital" (A6). These two views of the digital can be applied to some of the rights listed in Section B of Table 2, as rephrased and categorised in Table 3. The separation of these two different paradigms of the digital enables us to achieve a clearer view of digital rights according to different standpoints. One view seeks to adapt existing rights into a different space, and the other addresses "new" rights that focus on the centrality of digital data.

[8] One example from the literature can be seen in a paper by Remensperger et al. (2018) titled "Using research in digital rights advocacy", subtitled "Understanding the research needs of the Internet freedom community", implying that digital rights and Internet freedom are one and the same.

Table 3: Two Different Paradigms of "Digital" and Associated Rights

Digital as spaces	Digital as data representation of physical entities
□ Rights to freedom of expression, association and assembly online □ Right to consumer protection □ Right to seek joy and pleasure □ Right to exist free from violence, hateful speech, and harassment □ Right to not be discriminated □ Right to have informed consent on participation	□ Right to data privacy □ Right to freedom from digital surveillance □ Right to data ownership and control □ Right to data security and protection

There are certain rights mentioned that do not fall within the digital paradigms. These are rights that pertain to the access to, and the governance of the digital (see Table 4). Access and governance can be grouped together under a developmental paradigm, as access is one of the key concerns of information and communication technologies for development (ICT4D), and governance has to do with the contestations of power to define the direction of the development of digital environments.

Table 4: Two Different Paradigms of Digital Development and Associated Rights

Access to the digital	Governance of the digital
□ Right to access state and other services online □ Right to access the Internet □ Right to access information and content □ Right to access hardware/software	□ Right to participate in digital governance processes or be consulted on Internet policy issues

Four Spheres of Digital Rights

The framework proposed therefore includes four spheres, organised by two sets of paradigms as discussed in the previous section: the digital, and the developmental (See Table 5). The framework provides a structure to think about digital rights and is not a neat categorisation of each individual right; certainly, some rights may belong to more than one of the spheres. Through thinking about digital rights from these four spheres, we are able to draw from their respective areas of academic literature. From the data collected from the focus groups, it is also apparent that each sphere comes with its own implications and challenges. The following sections provide further elaborations. As one can dive as deeply into each sphere as one wants to, here I will only provide an idea of what the sphere entails as far as it makes sense within the scope of this paper, combining the insights from literature and from the data collected.

Table 5: Four Spheres of Digital Rights

Paradigm	Digital Paradigms		Developmental Paradigms	
Sphere	Conventional rights in digital spaces	Data-centred rights	Access to the digital	Governance of the digital
Description of sphere	Rights of individuals in digital spaces / on the Internet	Digital data that represents physical entities	Access to digital spaces and meaningful participation	Digital and Internet governance
Examples of rights	□ Rights to freedom of expression, association and assembly online □ Right to consumer protection □ Right to seek joy and pleasure □ Right to exist free from violence, hateful speech, and harassment □ Right to not be discriminated □ Right to have informed consent on participation	□ Right to data privacy □ Right to freedom from digital surveillance □ Right to data ownership and control □ Right to data security and protection	□ Right to access state and other services online □ Right to access the Internet □ Right to access information and content □ Right to access hardware/ software	□ Right to participate in digital governance processes or be consulted on Internet policy issues

Conventional Rights in Digital Spaces

It has been repeatedly mentioned, both on the ground and in academic works, that the UN Human Rights Council states that, “the same rights that people have offline must also be protected online” (Kumar et al., 2017). From the FGDs, it is clear that this forms much of the thinking of Southeast Asian advocates when they consider digital rights.

What are digital spaces? In 1996, John Perry Barlow[9] wrote a Declaration of the Independence of Cyberspace, considering "cyberspace" as a global, borderless, free, and liberated social space that is formed of "transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications, [...] a world that is both everywhere and nowhere, [...] a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth, [...] a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity."10 The romantic and idealistic description of a brave new world free from powers that be and structural constraints is further from reality than ever in the mainstream online world of today. Instead, with the advent of social media, linking our virtual identities with our real world connections, digital spaces can be seen as some sort of "digital togetherness" (Marino, 2015) in which people can connect in social spaces online which are not bound by geographical or time limitations but ultimately be rooted within socio-political and cultural structures of the physical world. It would be good to be reminded at this juncture that not all digital spaces are online – for instance, one's collection of electronic books in her e-book reader is within a digital space but may not be connected to the Internet.

In digital spaces, rights, as outlined by the UDHR, the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR), should still stand or be modified to suit the specificities of the spaces afforded by new technologies. While freedom of expression online is often singled out as representative in the set of rights that must be protected in the digital space, it is only one of the many rights under the UDHR, and these rights should be viewed as a system and not be divisible (Joergensen & Marzouki, 2015). At a different level, the UDHR, while often cited, is only one of the frameworks to organise rights. Discussions in the regional focus group pointed out that there are other frameworks that can be used, based on social justice, democracy, or feminist principles (see the Feminist Principles of the Internet11), for instance. As each framework would have its own limitations, the diversity of frameworks is not seen as a problem but to contribute to the overall discussion of what digital rights are.

It should be pointed out that digital spaces do not exist in a vacuum but are shaped by state and market forces. As expressed by respondents of the study, on one hand, Southeast Asians face challenges from the state, imposing draconian laws onto digital spaces. On the other hand, they are subjected to using online platforms which have community guidelines and moderation by tech companies which are culturally removed

[9] John Perry Barlow was an American poet, essayist, and political activist. He co-founded the Electronic Frontiers Foundation, one of the first digital rights organisations, and served on its board of directors until his death in 2018.

[10] The declaration was written in response to the enactment of the Communications Decency Act in the US. Full text accessible at https://www.eff.org/cyberspace-independence.

[11] See https://feministinternet.org/en/principles.

from the region and do not provide enough resources to handle issues such as cyber harassment or account hacking. Most of the digital spaces online, especially popular social networks sites, are developed and maintained by private entities such as Facebook. The platform features are designed by these companies, which have a disproportionate amount of control over how people communicate and engage with each other on their platforms, from a technical point of view (such as the algorithm that determines the news feed) or a policy point of view (such as the use of real names). Users have little say in these decisions and are compelled to play within the rules of the game if they want to be part of the network.

Besides considering state and non-state actors that dictate the rules of engagement in digital spaces, digital technologies themselves come with certain technological affordances which sometimes exacerbate wrongdoing. Doctoring images and spreading rumours, for instance, can be done with minimal cost and to great effect; something which could not be done in the pre-digital era. More sophisticated cyber attacks come in the form of hacking and taking over online presences, or seizing control of one's digital resources, or intercepting communication with surveillance tools. In certain cases, access to justice is hampered by the lack of capacity of law enforcement when it comes to digital rights issues. A discussion in one of the focus groups in Malaysia illustrates the point that, in certain cases, violations of rights online are not taken as seriously as offline violations. In a specific case, a woman who received multiple death and rape threats online had reported the case to the Malaysian police, whose first recommendation for her was to log off the Internet, implying that the threats sent to her would not affect her security if she did not read them. Upon deciding to pursue her case, she was instructed to sift through thousands of hate comments and profiles to capture the most salient attacks that would then be investigated by the police. This is not an isolated incident as other cases of online violence have been handled similarly, suggesting the police's reluctance or incapability to protect citizens' safety online.

Despite their shortcomings, digital spaces are still important spheres for exercising civil rights, especially in the situation of countries with closed civic spaces (Vietnam was given as an example) or marginalised, and persecuted communities (such as LGBTIQ communities in Malaysia). As digital spaces afford more freedom than physical spaces, these communities exercise their rights as much as they can within the digital spaces in order to expand the access to these rights within offline and analogue spaces.

Data-Centred Rights

"If you can make sure that the data that represents a person is protected in a way that it cannot be weaponised against him, you are essentially protecting the human rights of that person," said one of the respondents. This has been worded in a different way in the literature: by "turning citizens into data doubles," corporations and governments have been able to conduct "social sorting and alter access to resources and life chances, producing inequality and discrimination" (Hintz & Milan, 2018, p. 3943). The data representation of entities goes beyond individuals. Technological advances such as smart home applications enable us to build data models of homes to control their security and ambience; in smart cities there are sensors deployed or data collected in other ways to give us a treasure trove of data which can analyse and moderate traffic, air pollution, crime rates, and so on. Measurable characteristics and behaviour of physical entities are abstracted into data representations, enabling a multitide of usages with societal implications.

Data protection, security, and privacy therefore becomes the centre of this set of digital rights, with the understanding that digital technologies enable efficient collection and analysis of data, to "good" and "bad" ends. While we will not dwell on philosophical questions of what good and bad are, there are certain baseline agreements. Bad data practices have been observed to include mass gathering of data without transparency and accountability (sometimes illegally and unethically) and the increased use of that data in algorithmic decision-making, which involves the masses but is often opaque and unaccountable. Good data practices, on the other hand, protect and promote human rights and social justice towards achieving sustainable development (Mann, Devitt, & Daly, 2019).

The datafication of society has brought about implications at a global scale. For one, there is the use of data for surveillance both for the ends of corporate interests and state control. Surveillance capitalism (Zuboff, 2015) has emerged as a new form of market capitalism, set to surpass previous forms that were based on products and services, or financial markets and speculation. Zuboff explains that surveillance capitalism involves the following model: 1) companies push for more users and collect user data and data from users' online behaviour, 2) the data is analysed through artificial intelligence (AI) and machine learning, 3) these analysis are converted into products that predict human behaviour, and 4) prediction products are refined into products that convert human behaviour. As can be imagined, the ability to change human behaviour is highly coveted, and can have many consequences ranging from making sales to fixing elections. Hintz & Milan (2018) flatly state that data-based surveillance is a brand of "Western" authoritarianism in the digital realm that is institutionalised in law and normalised in society through popular culture, with implications no less powerful than "classic" authoritarian practices in targetting civil society and democratic institutions.

From a Southeast Asian perspective, some of the issues that were mentioned in the FGDs include the mass collection of citizen data through national identification and/or biometric systems, massive data breaches of citizen information, blanket and targetted digital surveillance, and the lack of public awareness of the importance of keeping their data safe and private. Data flows are transnational, as most popular services used are not local companies, with servers located all over the world. Respondents pointed out that users of the services have no control over their own data and how it is used by corporations. In almost all focus groups the threat of China was mentioned, not only in light of Chinese surveillance technologies and ideologies that are being pushed to authoritarian governments within the region, but also scepticism that Southeast Asian governments would have the abilities to protect their citizens' data against external surveillance by China.

At the national level, respondents offered insights of increased collection of citizen data by the state, through "objectifying the individual with numbers, whereby sometimes the numbers are more important than the individual", as put by a respondent. In the Philippines, the law to put in mandate the universal adoption of a national identification system is highly debated. On one hand, it provides the convenience of administering state services, but on the other hand a log is kept of where the ID holder has used the card, thus collecting and anchoring one's digital trail to one ID number. Advocates voiced their scepticism of the ability of the government to prevent data breaches. In the Thai focus group, a respondent opined that much of the state procurement of systems and technologies for mass collection of citizen data is vendor-driven, which is to say that the data is collected without any immediate goal and is not done in a critical manner. In Malaysia, concern was expressed on the imminent inclusion of one's mobile phone number into the information of one's national ID, which links different datasets by default, making it even easier to form a digital profile of the individual.

Access to the Digital

About 60% of Southeast Asia's population is connected to the Internet, with uneven access across the region, as shown in Table 6. The top four countries of Brunei, Singapore, Thailand, and Malaysia have more than 80% of their populations online, while the bottom three of Laos, Myanmar, and Timor Leste have only a third of their populations online. These figures have to be considered against the population size, as Indonesia with its vast population has more than 300 times the number of Internet users in Brunei, even if its Internet penetration is only 53.2%. Respondents pointed out that access is not only about basic infrastructural access but also about quality of service and affordability, as well as literacy in how to maximise the access to connectivity.

Table 6: Internet and Facebook Penetration in Southeast Asia

	Population (2019 est)	Internet users	Percentage of Internet users out of population	Facebook users (31 Dec 2018)	Percentage of Facebook users out of population	Percentage of Facebook users out of Internet users
Brunei	439,336	416,798	94.9 %	350,000	79.67%	83.97%
Singapore	5,868,104	4,955,614	84.5 %	4,300,000	73.28%	86.77%
Thailand	69,306,160	57,000,000	82.2 %	46,000,000	66.37%	80.70%
Malaysia	32,454,455	26,009,000	80.1 %	22,000,000	67.79%	84.59%
Vietnam	97,429,061	64,000,000	65.7 %	50,000,000	51.32%	78.13%
Philippines	108,106,310	67,000,000	62.0 %	62,000,000	57.35%	92.54%
Indonesia	269,536,482	143,260,000	53.2 %	130,000,000	48.23%	90.74%
Cambodia	16,482,646	8,005,551	48.6 %	6,300,000	38.22%	78.70%
Laos	7,064,242	2,500,000	35.4 %	2,200,000	31.14%	88.00%
Myanmar	54,336,138	18,000,000	33.1 %	16,000,000	29.45%	88.89%
Timor-Leste	1,352,360	410,000	30.3 %	390,000	28.84%	95.12%
Region-wide	662,375,294	391,556,963	59.11%	339540000	51.26%	86.72%

Source: Internet World Stats, 2019[12]

It can be seen in Table 6 that most of the Internet users in Southeast Asia are connected to Facebook. One observation that arose from a respondent was that social media was a main pull factor for much of Southeast Asia's population to connect to the Internet. According to the respondent, prior to the rise of social media, most of the digital rights work focused on information and communication technologies (ICT) for development (ICT4D), which is to see ICT as a public good, and champion issues along the lines of Internet access, digital economy, distance learning, etc. With the mass adoption of Internet connectivity and increased participation of the public and private sectors, the narrative of digital rights and funding priorities within civil society shifted towards a rights-based framework.

It is true that most of the discussions in the focus groups did not zero into Internet access, even if the data shows that there is still much room for improvement in connecting the

[12] https://www.internetworldstats.com/stats3.htm

region. This could be due to the fact that all of the focus groups were conducted in the major cities with high Internet penetration. Instead, access was discussed from some other levels, such as from the point of view of the right to access digital spaces and services. Sometimes access is blocked by the state in terms of Internet shutdowns or blocking of websites – an example of the latter was given of Malaysia's blocking of a fan fiction website, Fanfiction.net, which is popular among women and gender minorities as a space to explore creative writing and erotic literature. Sometimes access is not blocked, but is a result of negligence when entire communities are excluded because technologies are not designed to accommodate them. For example, automatic teller machines (ATMs) in Malaysia are currently not designed for the blind, and in the process of phasing out human bank tellers with ATMs, the blind's access to banking becomes increasingly difficult.

Discussions also brought up digital products and services that force the consent of the users in accepting the terms and conditions before they can access them. An example is the common practice of having to agree to all of the terms of use when participating on digital platforms or using certain devices, or otherwise lose access to the benefits offered by connectivity or a smart phone that one just bought. The principle of the matter is similar with another example provided by a Philippine respondent on his inability to apply for a passport, if he did not opt in for a national identity card, which in his perspective meant that he would have to provide his data in exchange for access to state services.

One more interesting example that arose from the discussions with regards to access is the case of *Free Basics*. Free Basics by Facebook is a free service for partial access to the Internet (to certain designated websites including Facebook) for communities that did not have access to the Internet before. In Southeast Asia, Free Basics is available in Cambodia, Indonesia, Laos, Philippines, Thailand, and Timor Leste13. It was pointed out in the context of the Philippines that users of Free Basics only read the headlines of links in their Facebook newsfeed, as they would have to pay to visit the actual pages linked. The unintended consequence of this partial access is the incentivisation of clickbait and misleading headlines, fuelling the spread of misinformation, as sensational headlines get shared even if the content of the article is of low quality or has nothing to do with the title. This issue falls under net neutrality, which is one of the many ways that the Internet can be fragmented into connectivity islands through technological developments, governmental policies, and commercial practices (Drake, Cerf, & Kleinwatchter, 2016). The next section on governance addresses issues like these.

Governance of the Digital

Beyond working on issues of access and driving digital innovation, the real challenge of the digital era is the governance of the digital. Digital governance, as defined by Floridi,

[13] https://info.internet.org/en/story/where-weve-launched/

is, “the practice of establishing and implementing policies, procedures, and standards for the proper development, use and management of the infosphere,” (2018, p.3) with the infosphere defined as, “that special place [...] that is seamlessly analogue and digital, offline and online” (Floridi, 2018, p.1). The main right, connected to the governance of the digital, is the right to participate in the governance processes that shape the digital space, to make policy decisions on issues that have been alluded to in the previous sections.

The governance of the digital is no simple matter, involving multiple state and non-state actors, from many layers. Governments perform certain governance functions such as regulating the industry and ensuring that digital technologies are used lawfully. In the private sector, risks of rights violations (in terms of freedom of expression and privacy rights) can happen across the entire value chain of the ICT industry, as mapped out by Hope (2011), who identified risk drivers across eight segments of the ICT industry[14.] Zooming into the governance of the Internet, an important subset of digital governance, a wide range of global players participate in the policy processes including the defining of protocols and standards and managing critical Internet resources15.

The wide-ranging issues of digital governance from human rights to cyberwarfare provide a dizzying number of possibilities for policy interventions. However, the policy directions differ depending on which vision of the digital one is working towards – there are at least four visions, according to the geopolitics of digital governance (O’Hara & Hall, 2018). There is the Silicon Valley view of an open and transparent Internet with data and software portability and interoperability, the European vision of a so-called “bourgeois” Internet where bad behaviour is contained and privacy is protected, the Chinese authoritarian Internet that holds extensive surveillance and regulation of citizens’ behaviour would ensure a harmonious society, and the Washington D.C. angle of protecting online resources and intellectual property for monetisation. Other proponents (countries pointed out are Russia, Iran and North Korea) exploit the openness and vulnerability of the Internet for misinformation and hacking, creating another dimension for the evolution of the Internet’s possible futures.

Southeast Asian digital rights advocates mainly work at national levels, such as mobilising to oppose draconian cyber crime laws, or providing input to local ICT policies. Beyond that, much of digital or Internet governance happen outside their sphere of influence, given that they are far removed geographically from the geopolitical centres or from tech companies that design, develop, and dictate the terms of use of online platforms and other digital technologies. Users have little say in how the companies that provide digital

[14] The eight areas are the following: 1) telecommunication services, 2) cell phones and mobile devices, 3) Internet services, 4) enterprise software, data storage, and IT services, 5) semiconductors and chips, 6) network equipment, 7) consumer electronics, and 8) security software.

[15] More information on these processes and participation mechanisms can be found in a guide by the Internet Society, accessible at https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-Internet-Ecosystem.pdf

spaces are run, "short of boycotting the product", as put by a respondent. Some digital rights advocates also view the rise of Southeast Asian tech companies with trepidation, pointing out that these companies are bound by data protection and privacy regulations of their own country, which the advocates view to be not as stringent as laws in developed countries.

The Digital Rights Movement in Southeast Asia

While scholars have written about various aspects of digital rights and related violations in Southeast Asia (e.g., Liu, 2014; Laungaramsri, 2016), the digital rights movement itself has not been documented much within the literature. This is the first such attempt to give a snapshot of the movement within the region, drawing from insights of national-level and regional-level digital rights advocates and activists within Southeast Asia. All of the following observations come from the FGDs unless otherwise stated.

There are eleven countries within Southeast Asia with varying levels of progress in their advocacy on digital rights. Naturally, the digital rights movement as a smaller subset of civil society within a country would reflect the characteristics of the country's civil society. From the impression of one of the respondents, the most active countries appear to be the Philippines, Indonesia, and Myanmar – groups have galvanised behind various digital rights issues and worked together on governance issues. In Thailand and Malaysia, there are pockets of activism happening, but mostly ad hoc and issues-based. Cambodia, Laos, and Vietnam as a cluster of countries have civil societies that are fractured; some segments are more closely aligned with the government, hence, there is limited resistance towards state violations of digital rights – there are champions of issues but not a movement per se. In Singapore, Brunei, and Timor-Leste, there is no perceived digital rights movement; while Singapore and Brunei have a weak civil society in general, Timor-Leste as the youngest country in Southeast Asia has a civil society that is focused on other developmental priorities.

There is not much of regional advocacy in terms of digital rights. Respondents have attributed the lack of a regional voice to some few factors. Firstly, as a region with diverse cultures and tongues, the digital rights movement faces language barriers in understanding what is happening in each country, which obstructs movement building. For instance, a non-Thai speaking respondent who lives in Thailand expressed that it is difficult to understand the dynamics of what is happening, as most of what is translated to English is just a summary. Another respondent asserted that a joint movement would have to first start at the national level and move on to the regional level because of the language barriers, as opposed to Latin America which can mobilise across borders in a more efficient manner, with fewer language-related challenges.

Secondly, there is no viable platform to advocate for digital rights issues at the regional level common to the Southeast Asian states. While there is the inter-governmental

Association of Southeast Asian Nations (ASEAN), there was unanimous agreement that ASEAN does not work well as a platform to champion for digital rights – the principle of non-interference in ASEAN[16] meant that any issue would be referred back to the national level. The lack of faith in ASEAN as a platform draws also from the discouraging experience of civil society in attempting to interface with the association for more than a decade, with not much to show as progress. The Asia Pacific Regional Internet Governance Forum (APrIGF)17 was mentioned as another platform to push new ideas at the regional level, however, it was pointed out by a respondent that governmental officials from Southeast Asian countries do not participate in that forum; even when they do speak on the panels they usually come in their individual capacities. This was contrasted with East Asian government representatives who do participate and defend their positions, which leads to a more fruitful engagement.

In terms of movement building across the region, a notable effort is the COCONET Southeast Asian Digital Rights Camp, held in Yogyakarta, Indonesia in October 2017 by EngageMedia, the Association for Progressive Communications (APC), and the Southeast Asian Press Alliance (SEAPA) with seven other partners18. The camp gathered 105 digital rights "experts, journalists, activists, artists, technologists, researchers and film-makers", about 80% of them from Southeast Asia, with 5-15 participants per country19. Some outcomes of the event were increased cross-country networks and collaborations at small scales but which are nonetheless important for a new movement. COCONET 2 is happening in November 2019, with a COCONET 3 planned within the pipeline.

Across all focus groups there was agreement that digital rights is not mainstreamed within the rest of civil society. Different issue areas are able to mobilise different sectors of civil society. For instance, media freedom groups are natural instigators or allies on freedom of expression online, and women and children's groups have a stake in online safety. However, digital rights as an umbrella issue attains scarce attention, as civil society focuses on their main mandates and priorities (such as environmental work, refugee and migrant issues, public health, etc.) that preceded the new and unfamiliar threats brought about by digital technologies.

[16] The principle stems from the notion of respecting the sovereignty of each member state to manage its own internal affairs, and has been enshrined within the Treaty of Amity and Cooperation in Southeast Asia of 1976.

[17] APRiGF is an annual conference to foster multistakeholder discussions on Internet governance at the regional level of Asia Pacific, and also serves as a platform to aggregate discussions of national Internet Governance Forums of countries within the region.

[18] Including Empower (Malaysia), Myanmar ICT for Development Organization (MIDO), SAFENET, and PurpleCode Collective (Indonesia), Thai Netizen Network, WITNESS, and the Cambodian Center for Human Rights.

[19] The outcomes report can be accessed here: https://www.engagemedia.org/CoconetShortReportFinal.pdf

Areas of work

As a comprehensive account of areas of work on digital rights would require a mapping exercise that goes beyond the scope of this study, this chapter provides some broad strokes of trends and observations gathered from the FGDs, which future work can build on. From the FGDs, there is agreement that the Southeast Asian civil society focus mostly on online freedoms of expression and information; somewhat due to reactions of civil society towards the encroachment of draconian laws into digital spaces. Media freedom organisations are equipped to deal with these issues, together with the existing clout of civil society championing for civil freedom issues. Another area that has been well-covered is online safety in the way of gender-based violence online, cyber-bullying and trolling, or digital security training for human rights defenders and marginalised communities. These issues tend to have a larger buy-in from the concerned publics because the narrative is clear cut and builds on legacy problems of the past. Other issues that have generated discussions within civil society include data collection and retention, due to massive data breaches; digital surveillance is an issue of concern but most point out that stories of surveillance are mainly anecdotal and based on hearsay, with no substantial evidence to base advocacy on. However, these discussions have not moved beyond civil society into mainstream public awareness.

Access to the Internet, as one of the earlier issues in terms of ICT for development, seems to have fallen out of favour when it comes to advocacy work, possibly due to a shift in funding priorities, but also because governments have taken over the responsibility to connect their citizens to the Internet. Some consumer groups had been working on quality of service and affordability in the past, as well as the free and open source software movement which sought to promote access to non-proprietary software, but these groups are not as active anymore within the region, or are disconnected with civil society that is more political. Overall, it seems that the discussion has shifted beyond basic access, to include issues, such as clear language in informed consent, digital literacy, and web standards for accessibility for people with disabilities.

In terms of issues of concern that are not addressed enough, technical attacks on civil society rank highly. These technical attacks come in the form of Distributed Denial of Service (DDoS) attacks, interception of data through fake cellphone towers (IMSI-catchers such as Stingray), supply chain attacks, and so on. Artificial intelligence and other ways of manipulating big data are also considered difficult and are scarcely discussed, when there are other immediate concerns that violate digital rights. In general, digital rights advocates find it difficult to advance in issues that are shrouded in state or corporate secrecy, such as surveillance, biometrics and national identification systems, organised astroturfing, arbitrary website or account take downs, and so on.

In terms of strategies employed for advocacy work, a wide range was mentioned, from policy advocacy to capacity building. All of the focus groups at the national level mentioned some form of engagement with governments, whether through consultations or through multistakeholder meetings such as Internet Governance Forums. Digital security trainings for human rights defenders or high risk and marginalised communities are common. In all of the countries within the sample, large scale online campaigns have been organised against draconian law-making, affecting digital rights, such as Thailand's fight against the amendments of the Computer-related Crime Act which garnered more than 300,000 petition signatures (according to figures by Human Rights Watch (2016), even though a respondent put the figure at 370,000)), Malaysia's Internet Blackout Day against Section 114A within the Evidence Act (Cheong & Yeap, 2012), and the Philippines in their crowdsourcing of a Magna Carta for Philippine Internet Freedom in opposition to the Cyber Crime Act 2012 (York, 2013). In most of these instances, the campaigns were successful in generating public awareness and conversations, even if many did not lead to a change in policy direction. There has also been work on protecting civil society with technical support and defense, as well as attempts to link civil society with tech communities, even though these areas of work are limited compared to other areas.

Challenges Faced

In terms of challenges that are specific to digital rights work, an oft-mentioned one is the lack of understanding of the topic, within civil society and also by the general public. Within civil society, digital rights work has an "inconsistent constituency", according to one of the respondents. As people do not completely understand what digital rights is, participation in the advocacy is ad-hoc and reactive, based on issues that crop up. Change is difficult to sustain without a strong core movement, and when resources within civil society are spread thin. There is a "sheer lack of digital rights activists" - on one hand, some advocate on digital rights issues without seeing themselves as advocates for digital rights, and on the other hand digital rights issues are fragmented, and those who are working on specific issues (for instance, online gender-based violence) without identifying with the larger movement end up working with the same people repeatedly, without connecting their work with other issues such as data collection and retention.

On top of that, the lack of digital literacy within the wider circle of human rights defenders means that activists continue to use third party platforms with problematic privacy and data policies, inadvertently contributing to corporate and state surveillance; lax attitudes towards personal and organisational digital security also mean that they would compromise themselves and their stakeholders if their devices or systems are compromised. Without a clear understanding of digital rights, human rights defenders and their funders end up perpetrating practices such as the indiscriminate collection of stakeholder data without a data retention policy or a data security plan.

Digital rights advocates find it difficult to communicate their work, which compounds the problem of the lack of awareness in the general public. Sometimes the issues do not bring immediate consequences and are just potential violations that may happen in the future, such as the case of indiscriminate data collection vulnerable to future data breaches, which makes it difficult to generate support for the cause. Digital rights activists tend to "shortcode" their communication with underlying assumptions (such as the value of privacy or the importance of data protection) which may not relate to stakeholders outside of the movement. The result adds to the silo effect and digital rights advocates end up preaching to the choir, reaching those who are already converted – as the general public continues to overshare on social media and give out their personal information without much concern.

Even within the digital rights movement, there is a lack of technical expertise, as most of the advocates come from civil society and not from a technical background. There are a few organisations that work with or are run by tech professionals, but more often than not digital rights issues are taken up as programmes and focal areas by organisations which have an interest in certain areas but may not have the technical capacity to deal with the digital aspect of digital rights. As such, advocacy work stagnates at a level of obtaining the low hanging fruits such as conducting digital security training workshops (through outsourcing to a small pool of available trainers) or networking events on topical issues. When digital rights violations include technical attacks, civil society does not have the capabilities of defense or offense.

Language barriers also affect digital rights work. At one level, English is the main language used for cross-border work. Those who do not speak the language will find themselves at a disadvantage, whether during civil society forums at the regional or international level, dealing with platforms such as Facebook when reporting problems, or when accessing digital security helplines set up by international NGOs. Participation in Internet or digital governance is even harder when language-related barriers include technical jargon that even good English speakers would have difficulties understanding. At another level, even within countries themselves there is a diversity of languages being used, fragmenting communication.

On access to funding, there are mixed responses. On one hand, it is acknowledged that digital rights as a field has been attracting donor funds in the past five years and will probably continue to do so, as more and more people get connected to the Internet and human rights violations in digital spaces continue to mount. On the other hand, CSOs appear to have difficulties accessing these funds. An example given by respondents in Thailand is that sometimes the funding is offered in an amount that surpasses the managerial capacity of smaller organisations to manage, therefore placing the funds beyond their reach. Another point mentioned in the Malaysian group is that funding for digital rights is usually project-driven and core funding is few and far between, making it difficult for organisations to run their day-to-day operations and pay living wages to their staff. In the Philippines, it was mentioned that the lack of resources makes it difficult to acquire new technologies, to test, experiment, and learn on.

On challenges faced by digital rights advocates that are common to the wider Southeast Asian civil society, these include difficulties in registering and running an organisation, politics within civil society, and the narrowing civic space in general. Organisations that are not registered then lose access to funding as well due to most funders' policies to give only to registered organisations. Civil society organisations get entrenched in the issues that they set out to solve and that they already have expertise in. There is often no exit strategy or resources to move to newer issues, hence, the adoption of digital rights issues is slow. In general, smaller local civil society organisations are often personality-driven, with weaker institutions compared to their corporate counterparts, and fail to attract good talent.

A respondent opined that people in the region are more interested in bread and butter issues, relegating civil freedoms to a lower priority – making the promotion of digital citizenship or the rights and responsibilities of being a citizen in the digital space even harder. A bottom-up approach in pressuring the governments to change the law based on principles of civil freedoms is therefore very difficult, whereas issues framed from an economic point of view would be much better received.

Recommendations to Improve the Digital Rights Movement

There are a number of recommendations that digital rights advocates offer as what would improve the movement in Southeast Asia, as follows:

- *To communicate the relevance of digital rights issues to the wider civil society and other stakeholders.* It was mentioned often that digital rights activism happens in silos and that the same faces appear in the same issue-based forums repeatedly. The concerns of digital rights activists should be conveyed to the wider civil society in a manner that would relate the issues to the stakeholders – for example, case studies on digital rights need to frame violations in a manner and language that would be understandable and relatable to the general public. Advocates should also reach out to communities who are likely to be sympathetic towards digital rights issues, such as activists who are power users of social media for their causes, or communities who are interested in digital media, such as hackers, gamers, or free and open source software enthusiasts.

- *To push for a wider education of digital literacy and digital rights to the public.* Although digital technologies are now widely taught in universities and schools, most of the lessons focus on the application of the technologies and not deeper issues such as philosophy and politics of technology. In corporating these overlooked perspectives, the younger generation can be inculcated to think more critically about the impacts of technology use. It is also vital to educate the older members of the public who tend to be holders of power and policymakers on these issues or those who tend to be less savvy in using technology in a safe and responsible manner.

- *To have more movement building and collaborations at the regional level.* This would bring multiple benefits, such as knowledge transfer and capacity sharing, and soliciting support from the international community when individual countries are facing crises. It was also mentioned that governments within the region learn from each other in terms of authoritarian measures, and so digital rights advocates should form networks to collaborate. While there are some individuals within the Southeast Asian region with the knowledge and experience in participating in Internet governance forums, this knowhow needs to be mainstreamed within the movement for effective policy change.

- *To increase the involvement of the tech community within the digital rights movement*. The gap between the digital rights movement and the tech community needs to be bridged, as the expertise from the tech community is much needed to provide the movement with the knowledge of the technicalities of digital rights, technical support upon cyber attacks, and tools to facilitate some digital rights work, such as apps to combat fake news, or to maintain connectivity when mobile signals are jammed during demonstrations. For this to happen, there has to be more outreach to the tech community to sensitise them for human rights, and to entice them to contribute their skills into the area. The case of Taiwan was given as an example of active involvement of hacktivists in its digital rights movement, who have the combination of the technical skills and understanding of social issues.

- *To increase the technical capacity within the digital rights movement*. For some digital rights issues, especially technical topics such as data security on various technologies, technical experts are needed to analyse the societal implications of technology. At the moment, even though there are organisations doing some work in this area, the lack of technical expertise is a major gap within the region to propose or oppose policy directions. The digital rights movement needs tech professionals for more policy research, advocacy and recommendations, as well as to conduct more workshops and capacity building within civil society. Organisations should hire their own technical personnel, which would then be a basis of putting together a collective of technical professionals within civil society. Another suggestion was for civil society organisations to organise themselves into a membership organisation or cooperative which offers support for technical needs.

- *To improve access to funding*. Funding structures need to be diversified to include core or operational funding. Regional or bigger organisations can work on obtaining big grants and subsequently breaking it down to sub-grants to channel funding to local partners. Funders should also work on simplifying reporting, and understand that some aspects of digital rights work, such as building digital literacy, are long term efforts which may not have immediate impacts that can be measured. The reality on the ground is that many Southeast Asian digital rights activists do not register their organisations because of overly burdensome requirements, hence, barring them from receiving funding – an aspect that should also be considered by funders.

- *To support digital rights organisations with capacity-building on the administrative and financial management aspects of running their organisations.* As new organisations are being set up to advocate for digital rights as an emerging issue, these organisations need support and training in terms of managing projects, human resources, cash flow, and so on. Incubators have been suggested, or even the pooling of secretarial resources, in order to ease organisations from administrative bureaucracy and enable them to focus on their advocacy work.

- *To increase the amount of research and documentation that originate from within the region.* Although there are reports generated by international organisations which touch on the realities within the region (such as the *Freedom on the Net* report by Freedom House), there is a lack of regional-based reports and studies that focus on improving digital rights advocacy in terms of concrete strategies. Homegrown research would be able to better incorporate Southeast Asian cultural and political contexts, as well as the perspectives of regional activists into strategy-building. It was also mentioned that those who attend international conferences should bring the insights back to the local communities in order to build capacity, whether in the form of reports or presentations.

- *To seek out more platforms for the mainstreaming of digital rights.* National Human Rights Institutions (NHRIs) at the country levels were mentioned as potential platforms for mainstreaming, and also the ASEAN Intergovernmental Commission of Human Rights (AICHR). Free trade agreements and their negotiations may be good transborder platforms to champion digital rights. Also somewhat overlooked by Southeast Asian digital rights advocates are multistakeholder platforms such as the Internet Society, the Internet Corporation for Assigned Names and Numbers (ICANN), or the Internet Engineering Task Force (IETF), mainly from the perspective of inserting digital rights into web standards and hard coding ethical considerations into the Internet's architecture.

Conclusion

Many of the challenges within the digital rights field in Southeast Asia stem from the lack of a conceptual understanding of what digital rights is. Without a clear vision of the big picture, the movement ends up being fragmented into silos working on individual issues instead of working across issue areas to generate greater support. Advocacy is reactive instead of proactive due to the lack of a coherent framework to support strategy. Communication of problematic issues to the wider civil society and the general public is also weakened, leading to a slow growth of the movement itself.

The conceptual framework proposed within this paper aims to address the gaps mentioned. From the focus group discussions conducted with digital rights advocates, four spheres of digital rights arose: two that were based on different ways of viewing the digital (as spaces, or as data representation of physical entities), and two that were based on developmental angles of access and governance. It is found that Southeast Asian digital rights work centres on addressing many of the digital rights that pertain to conventional rights translated to digital spaces, through existing movements on civil freedoms. There is an increasing focus in the spheres of data-centred rights and digital governance, while work on access is shifting beyond basic Internet access and is more concerned about the quality of access. As most of the digital rights advocates originate from civil society rather than the tech community, technical capacity is sorely lacking, limiting most advocacy work to awareness campaigns rather than more technical aspects of the different spheres of digital rights, such as technical measures against cyber attacks, or data protection from a software architectural point of view. Participation in digital governance at a technical level, such as in the development of standards, is also difficult.

The digital rights movement studied is situated within the context of Southeast Asia and subjected to existing social, political, and cultural contexts. Difficulties in civil society work manifest within the microcosm of digital rights work – in the face of authoritarian governments, tight resources within civil society, and publics that are more concerned about economic development than rights violations. Although there is movement building at the regional level, most of the digital rights work in the region focus on the national level. While advocates are concerned about the transnational implications of geopolitics and powerful tech companies based in the West, the lack of resources, networks, and capacity limits their work in these aspects, with only a small number of familiar faces working in the international arena.

It is hoped that this paper will provide a strong basis for future research, whether to apply and refine the conceptual framework to other regions and localities, or as a baseline to deepen the understanding about digital rights work in Southeast Asia. As more and more of the world's population joins the global networked society, protecting and upholding digital rights will remain to be a salient issue for the foreseeable future. Perspectives and insights from the developing world will contribute to advocacy and research to ensure a safer, more equitable, and rights-based digital environment for all.

References

Cheong, D. D., & Yeap, S. Y. (2012, August 31). Malaysia's internet blackout: politicisation of online activism? *East Asia Forum*. Retrieved from https://www.eastasiaforum.org/2012/08/31/malaysias-internet-blackout-politicisation-of-online-activism/

Daskal, E. (2018). Let's be careful out there …: how digital rights advocates educate citizens in the digital age. *Information, Communication & Society*, 21(2), 241–256. https://doi.org/10.1080/1369118X.2016.1271903

Dheere, J. (2017). A methodology for mapping the emerging legal landscapes for human rights in the digitally networked sphere. In *Global information society watch 2017. Unshackling expression: a study on laws criminalising expression online in Asia* (Special edition, pp. 6–17). India: Association for Progressive Communications (APC).

Drake, W. J., Cerf, V. G., & Kleinwatchter, W. (2016). *Internet Fragmentation: an overview* (p. 80) [Future of the Internet Initiative White Paper]. Geneva: World Economic Forum.

Floridi, L. (2018). Soft ethics and the governance of the digital. *Philosophy & Technology*, 31(1), 1–8. https://doi.org/10.1007/s13347-018-0303-9

Gilbert, C., & Benedict, J. (2018). People power under attack: A report based on data from the CIVICUS Monitor. In *Forum-Asia Working Paper Series, Asian Perspectives on International Human Rights Landscapes*: *Vol. No 5, December 2018. Civic Space: challenges and ways forward*. Bangkok, Thailand: Asian Forum for Human Rights and Development.

Gill, L., Redeker, D., & Gasser, U. (2015). *Towards digital constitutionalism? Mapping attempts to craft an internet bill of rights* (Research Publication No. 2015–15). Berkman Klein Center for Internet and Society.

Global Network Initiative. (2017, May). *GNI principles on freedom of expression and privacy*. Retrieved from https://globalnetworkinitiative.org/gni-principles/

Hintz, A., & Milan, S. (2018). "Through a Glass, Darkly": everyday acts of authoritarianism in the liberal west. *International Journal of Communication*, 12, 21.

Hope, D. A. (2011). *Protecting human rights in the digital age* [Occasional Paper]. Retrieved from https://www.bsr.org/reports/BSR_Protecting_Human_Rights_in_the_Digital_Age.pdf

Human Rights Watch. (2016, December 21). Thailand: cyber crime act tightens internet control. Retrieved from https://www.hrw.org/news/2016/12/21/thailand-cyber-crime-act-tightens-internet-control

Internet Rights & Principles Coalition. (2018). *The charter of human rights and principles for the internet* (No. 5th Edition). Internet Rights and Principles Dynamic Coalition, UN Internet Governance Forum.

Joergensen, R. F., & Marzouki, M. (2015). *Reshaping the human rights legacy in the online environment*. 17–33.

Kumar, P., Prasad, R., & Maréchal, N. (2017). *Progress and peril: the role of ICT companies in promoting and curtailing human rights*. 26.

Laungaramsri, P. (2016). Mass surveillance and the militarization of cyberspace in post-coup Thailand. *Austrian Journal of South-East Asian Studies*, 9(2), New Media. https://doi.org/10.14764/10.aseas-2016.2-2

Liu, Y. (2014). Transgressiveness, civil society and internet control in southeast asia. *The Pacific Review*, 27(3), 383–407. https://doi.org/10.1080/09512748.2014.909520

Mann, M., Devitt, S. K., & Daly, A. (2019). What is (in) good data? In A. Daly, S. K. Devitt, & M. Mann (Eds.), *Good Data*. Amsterdam: Institute of Network Cultures.

Marino, S. (2015). Making space, making place: digital togetherness and the redefinition of migrant identities online. *Social Media + Society*, 1(2). https://doi.org/10.1177/2056305115622479

O'Hara, K., & Hall, W. (2018). *Four internets: the geopolitics of digital governance* (CIGI Papers No. 206). Retrieved from https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance

Redeker, D., Gill, L., & Gasser, U. (2018). Towards digital constitutionalism? mapping attempts to craft an internet bill of rights. *International Communication Gazette*, 80(4), 302–319. https://doi.org/10.1177/1748048518757121

Remensperger, J., Schwartz-Henderson, L., & Cendic, K. (2018). *Using research in digital rights advocacy: understanding the research needs of the internet freedom community*. Annenberg School for Communication at the University of Pennsylvania, Pennsylvania: Internet Policy Observatory.

UNESCO. (2015). *Principles for governing the Internet: a comparative analysis* (UNESCO Series on Internet Freedom No. 6). Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000234435

Van Tassel, J. (2016). *Digital Rights Management: Protecting and Monetizing Content*. Oxford: Focal Press.

York, J. (2013, July 8). *A brief analysis of the magna carta for Philippine internet freedom*. Retrieved from

https://www.eff.org/deeplinks/2013/07/brief-analysis-magna-carta-philippine-internet-freedom

Zuboff, S. (2015). *Big other: surveillance capitalism and the prospects of an information Civilization* (SSRN Scholarly Paper No. ID 2594754). Retrieved from https://papers.ssrn.com/abstract=2594754