Big Brother's Grand Plan: A Look at the Digital Security Playbook in the Philippines

Jessamine Pacis

Civic Futures

May 2023 civic-futures.org

Acknowledgments

This paper was written by an independent human rights researcher and activist in the Philippines under the Civic Futures initiative. It was supported by the **Fund for Global Human Rights** and **Active Vista Center Inc.** and edited by **Paulynn Sicam**.

About the Author

Jessamine Pacis is a researcher, writer, and digital rights advocate from the Philippines. She has a bachelor's degree in Broadcast Communication and Juris Doctor credits from the University of the Philippines.

From 2016 to 2022, Jess was a Program Officer for Privacy and Data Protection at the Foundation for Media Alternatives (FMA), a non-government organization in the Philippines that seeks to democratize information and communication systems for citizens and communities. She worked primarily in the topic of Privacy and Surveillance, and was also involved in projects related to internet governance and open data, as well as a research project that explored online domestic work platforms in the Philippines. The study looked at how digital care work or domestic work platforms are transforming traditional models of labor and power relations in the Philippine context, and examined whether such emerging models improve inclusion or merely reinforce existing inequalities. From 2019 to 2022, she was in charge of a policy advocacy project on cybercrime and cybersecurity policy. She has contributed articles and op-ed pieces to *CNN Philippines Life*, *Bot Populi*, and *GMA News Online*.

She attended the Asia Pacific School on Internet Governance and participated in the global Cyber capacity building program hosted by Global Partners Digital.

The author would like to thank the following organizations, human rights defenders, and academe, including those not listed for their safety and security, for their review and feedback on first draft of the research:

Foundation for Media Alternatives (FMA)

iDefend

KARAPATAN

Karl Arvin F. Hapal - Assistant Professor
College of Social Work and Community Development
University of the Philippines, Diliman

National Union of Peoples' Lawyers (NUPL)

No Box Philippines

Philippine Alliance of Human Rights advocate (PAHRA)

Resbak

Ria Landingin, Lunas Collective

Ritz Lee Santos III

The Women's Legal and Human Rights Bureau, Inc., (WLB)

Abbreviations and Acronyms

ATA	Anti-Terrorism Act of 2020
ATC	Anti-Terrorism Council
CCTV	Closed-circuit television
CICC	Cybercrime Investigation and Coordinating Center
COVID-19	Coronavirus Disease 2019
CPA	Cybercrime Prevention Act
CPP-NPA-NDF	Communist Party of the Philippines-New People's Army-National Democratic Front
DDoS	Distributed Denial of Service
DICT	Department of Information and Communications Technology
FICS	Funders Initiative for Civil Society
IMSI	International Mobile Subscriber Identity
IOC	Intelligent Operations Center
ISP	Independent Service Providers
LGBTQ	Lesbian, Gay, Bisexual, Transgender, and Queer
NCSP	National Cybersecurity Plan
NTC	National Telecommunications Commission
NTF-ELCAC	National Task Force to End Local Communist Armed Conflict
OEWG	Open Ended Working Group on security of and in the use of information and communications technologies
OSG	Office of the Solicitor General
PDRs	Philippine Depositary Receipts
PhilSys	Philippine Identification System
SEC	Securities and Exchange Commission
SIM	Subscriber Identity Module
SMS	Short Message Service
UN	United Nations

Source: Keith Bacongco, Flickr, CC BY 2.0 'Useless'.

I. Summary

The Philippines is a highly connected nation. Previously known for its high SMS use and now for its high social media use, the role of digital spaces in Filipinos' exercise of their civic freedoms is undeniable. However, numerous governance structures, laws and policies, and government activities pose threats to these civic freedoms in the digital environment. In the Philippines, surveillance, censorship, and disinformation are some of the most pressing of these threats. These were reinforced further by the unexpected massive shift to digital modes of public participation during the COVID-19 pandemic. Philippine civil society is pushing back against this digital security playbook through strategies, both old and new, asserting their own visions of safety and security in both offline and online spaces.

II. Introduction

On 10 October 2022, President Ferdinand Marcos Jr. signed into law Republic Act No. 11934 or the SIM Card Registration Act, the first law passed after he assumed office as the President of the Philippines. The law requires all Filipinos to register their SIM cards in an effort to combat SMS-based scams and other forms of fraud. Marcos Jr. also had an unlikely solution to the rising prices of petroleum — to implement the country's new national ID system. These measures might seem oddly placed in the eyes of an outsider, but they give an accurate indication of the Philippine government's attitude towards the internet and other data-intensive technologies. This research paper looks at the current state of Philippine digital spaces, how State and non-State actors have shaped definitions of and narratives about "cybersecurity," and how human rights figure into such definitions. It also looks at current threats on civic space, particularly those that take place in digital spaces. Finally, the paper investigates how civil society actors have resisted these through creative and innovative strategies and alternative narratives of security.

By way of limitation, while we look at the broader developments in cybersecurity and internet governance across history, this research is focused on the links between digital technologies and shrinking civic space in the Philippines during the Duterte administration (2016-2022).

The first part of this paper describes the global governance structures that affect security in cyberspace, and how the characteristics of Philippine internet and local policies shape the relationship between cybersecurity and civic space. The second section zeroes in on three major threats to civic space in relation to technology: surveillance, censorship, and disinformation. The last section highlights the forms of resistance and alternative meanings and manifestations of security that we have seen among local communities and lists several possible points of entry towards a new strategy of resistance. Weaved through all these sections is a probe into the different actors that drive key policies and programs related to internet governance and cybersecurity, and their respective motives and narratives.

III. History and Evolution of the Philippine Internet

The internet and other digital technologies have revolutionized the ways by which people participate in civic space.[1] Further, people's relationship with the internet varies across cultures, and Filipinos, in particular, have a very unique perception and use of the internet, which first needs to be examined before we look at what civic space looks like online.

Even prior to the boom of social media, Philippine civil society was already making use of ICTs to build social movements and amplify protests. SMS played a very important role in the mobilization of the Filipino public for the removal of former President Joseph Estrada in 2001 in what some writers referred to as a "coup d'text."[2] So high was the SMS usage of Filipinos in the late 1990s to 2000s that, for several years, the Philippines was known as the "texting capital of the world".[3]

Technology also played an important role in the massive call for the ouster of former President Gloria Macapagal-Arroyo in 2005, which stemmed from a leaked recording of Arroyo's conversation with Commissioner Virgilio Garcillano, a member of the Commission on Elections, which revealed a plan to rig the results of the 2004 presidential elections in favor of President Arroyo. Part of the leaked conversation was made into a mobile phone ringtone that was downloaded 350,000 times and was reportedly used by one million Filipinos during the height of the controversy.[4]

1 Institute of Development Studies, "Digital Rights in Closing Civic Space: Lessons from Ten African Countries," February 2021, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/15964/Digital_Rights_in_Closing_Civic_Space_Lessons_from_Ten_African_Countries.pdf?sequence=4&isAllowed=y

2 Raul Pertierra, "The New Media, Society & Politics in the Philippines," 2012, https://library.fes.de/pdf-files/bueros/asia-media/09241.pdf

3 Emil Tapnio and Steven Rood, "Social Media in the Philippines is Widespread, but what is its Impact?," October 12, 2011, https://asiafoundation.org/2011/10/12/social-media-in-the-philippines-is-widespread-but-what-is-its-impact/

4 Pauline Macaraeg, "LOOK BACK: The 'Hello, Garci' scandal," *Rappler*, January 5, 2021, https://www.rappler.com/newsbreak/iq/look-back-gloria-arroyo-hello-garci-scandal/

The Philippines connected to the internet for the first time in March 1994. The country was a late adopter to the internet compared to its Asian neighbors, and internet access in the country took a long time to develop due to a conflation of factors, such as the challenge of distributing equal infrastructure to different parts of the country, and corruption in the government.[5]

But today, almost 30 years after the Philippines first went online, Filipinos have come to be known as the biggest social media users in the world. The penchant of Filipinos for social media began in the early 2000s when the social networking website Friendster was introduced. At one point, Friendster became the most-visited site in the Philippines and eventually, in other Southeast Asian countries.[6] What was once the texting capital of the world, is now the social media capital of the world.[7]

We Are Social's Digital 2022 report says that Filipinos are the second biggest internet users in the world in terms of the average amount of time spent daily using the internet. This may not be surprising to most people, as the Philippines has been known for its widespread use of social media for years. What might be surprising to some, however, is the fact that based on the same report, in January 2022, there were only 76.01 million internet users but 92.05 million social media users in the country. There were even more Facebook users (83.85 million) than internet users in the Philippines in the same period.[8]

This "Facebook-first" internet access may have been a product of various reasons, but it is clear that such behavior is further encouraged by the way internet access is made available and accessible to Filipinos. In 2015, the Free Basics program was introduced by Facebook in the Philippines through the country's two major telco companies, Smart and Globe. The service allows users to load certain websites featured by Free Basics without incurring mobile data charges. This includes Facebook Free, which allows users to browse and post on Facebook for free without seeing photos or videos (i.e., free users can only view the text in Facebook posts). Users of this service are not able to access external content either. Hence, when viewing a posted link on their newsfeed, they can only read the headline, but they cannot view the thumbnail image or click on the link to read the full content. This phenomenon is widely known as a "walled garden," a limited and curated space that users may confuse to be the entirety of the internet. Proponents of similar services argue that it is a way to make the internet more accessible and affordable to people in countries with a great digital divide, but the negative effects of reliance by users on a single platform has been documented all over the world.[9] Such selective accessibility, and the dependence of a large sector of the population on this more affordable alternative, is believed to have facilitated the successful propagation of Duterte's anti-drug and anti-crime rhetoric,[10] along with other strategies such as the deployment of paid troll armies and social media influencers that consistently and strategically pushed Duterte's narratives on how the war against drugs is a pressing security concern.

5 Center for Information & Society, "Philippines – Public Access Landscape Study," archived September 27, 2013 at the Wayback Machine, https://web.archive.org/web/20130927181734/http:/faculty.washington.edu/rgomez/projects/landscape/country-reports/Philippines/1Page_Philippines.pdf

6 Sasha Lim Uy, "Did Filipinos Literally Love Friendster to Death?," *Esquire*, June 15, 2018, https://www.esquiremag.ph/culture/tech/filipinos-killed-friendster-a00204-20180615-lfrm

7 Janvic Mateo, "Philippines still world's social media capital – study," *The Philippine Star*, February 3, 2018, https://www.philstar.com/headlines/2018/02/03/1784052/philippines-still-worlds-social-media-capital-study

8 Digital 2022: The Philippines," DataReportal, last modified February 15, 2022, https://datareportal.com/reports/digital-2022-philippines

9 Sheera Frenkel, "This Is What Happens When Millions Of People Suddenly Get The Internet," *BuzzFeed News*, November 20, 2016, https://www.buzzfeednews.com/article/sheerafrenkel/fake-news-spreads-trump-around-the-world#.ca8ZvKzrQ

10 Davey Alba, "How Duterte Used Facebook To Fuel The Philippine Drug War," *BuzzFeed News*, September 4, 2018, https://www.buzzfeednews.com/article/daveyalba/facebook-philippines-dutertes-drug-war

IV. Cyber Policy and Governance

Since the early iterations of what we now know as the internet began to be developed in the 1960s, digital and virtual spaces have become major platforms where people all over the world exercise their civic freedoms, regardless of whether the same freedoms are respected or restricted in the state they reside in. Because the internet is a network of networks with no real center of power, there is no single entity that controls or governs it. Instead, internet governance involves various stakeholders such as governments, intergovernmental organizations, the private sector, the technical community, and civil society. Still, there are international treaties and cyber norms that serve as frameworks for acceptable behavior in digital spaces.

A. Global Cyber Policy

The most relevant international agreement in this area is the Convention on Cybercrime, also known as the Budapest Convention.[11] The Philippines' own cybercrime law is based in the Budapest Convention, albeit with several controversial additions.

At the time of writing, the United Nations is in the process of discussing a new cybercrime treaty that can completely change the way states behave in relation to each other in cyberspace. The treaty, first proposed by Russia, is presumably set to replace the Budapest Convention, which the Philippines' own cybercrime law is based on. The proposed treaty has been widely opposed since the beginning by digital rights organizations because of its treatment of cybercrime being extremely vague and open to abuse.[12] A key point of contention in these deliberations is the very nature of what constitutes a cybercrime. Cybercrime policy makes a distinction between "cyber-dependent" and "cyber-enabled" crimes. There is also concern among some states that the treaty might end up breaching the issues of national security, cybersecurity, or cyberwarfare on top of cybercrime.[13]

Cyber norms, on the other hand, come in the form of multilateral documents, multistakeholder statements, and outcome documents of multilateral forums. On top of being rare, international processes for setting cyber norms such as the Open Ended Working Group on security of and in the use of information and communications technologies (OEWG) of United Nations (UN) member states and the UN Group of Governmental Experts also remain largely inaccessible to and exclusive of civil society voices.[14]

11 "The Budapest Convention (ETS No. 185) and its Protocols," Council of Europe, accessed December 15, 2022, https://www.coe.int/en/web/cybercrime/the-budapest-convention

12 Deborah Brown, "Cybercrime is Dangerous, But a New UN Treaty Could Be Worse For Rights," Human Rights Watch, August 13, 2021, https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights

13 Katitza Rodriguez and Meri Baghdasaryan, "UN Committee To Begin Negotiating New Cybercrime Treaty Amid Disagreement Among States Over Its Scope," *Electronic Frontier Foundation*, February 15, 2022, https://www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among

14 Sheetal Kumar, "The missing piece in human-centric approaches to cybernorms implementation: the role of civil society," *Journal of Cyber Policy 6*, no. 3 (2021): 375-393, https://doi.org/10.1080/23738871.2021.1909090

There is no universally accepted definition of cybersecurity. Unlike cybercrime, which is addressed by an international treaty called the Budapest Convention, there is no international instrument that governs matters relating to cybersecurity. States, therefore, are given free rein on how they define cybersecurity, as well as the structures and mechanisms they create to ensure it. Most cybersecurity policies follow the definition by the International Communications Union as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and organization and users' assets."[15]

However, human rights advocates and civil society groups all over the world raise the danger of this systems-centric approach to cybersecurity being used to justify policies and protocols that are repressive and violative of civic freedoms. A recent joint civil society statement to the UN General Assembly's First Committee on Disarmament and International Security raised concern over the increase in offensive cyber capabilities and the use of cyber mercenaries among states. The statement points to the rising "toll of unrestrained cyber operations on human security" that makes it necessary for relevant UN processes to be guided by human-centric and rights-based approaches rather than securitized approaches that abuse cybersecurity laws, policies, and practices to violate human rights and fundamental freedoms.[16]

An alternative definition of cybersecurity proposed by the Freedom Online Coalition uses the same core principles as the one used by the International Organization for Standardization but puts the rights and safety of people at the forefront of cybersecurity, thus: "Cybersecurity is the preservation — through policy, technology, and education — of the availability, confidentiality, and integrity of information and its underlying infrastructure as to enhance the security of persons both online and offline."[17]

15 Tim Maurer and Robert Morgus, "Compilation of Existing Cybersecurity and Information Security Related Definitions," *New America*, https://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/

16 "Joint civil society statement on cyber peace and human security," Association for Progressive Communications, last modified October 17, 2022, https://www.apc.org/en/pubs/joint-civil-society-statement-cyber-peace-and-human-security-0

17 Why Do We Need a New Definition for Cybersecurity?," Freedom Online Coalition, last modified September 2015, https://freedomonlinecoalition.com/blog/why-do-we-need-a-new-definition-for-cybersecurity/

B. Philippine Cyber Policy

In the Philippines, the Department of Information and Communications Technology (DICT) was created in 2016 by virtue of Republic Act No. 10844. Included in the law is the creation of the Cybercrime Investigation and Coordination Center (CICC), which is tasked to formulate the National Cybersecurity Plan (NCSP), which shall set the direction for cybersecurity in the country for a period of five years. What is curious, however, is that although the CICC is named as a *cybercrime* center, the law makes no mention of cybercrime when describing the mandates of the office, but instead refers to *cybersecurity*. These are two entirely different things that are often interchanged. While cybercrime is defined as a computer-enabled or -facilitated offense punishable by law, cybersecurity refers to the tools and practices used to protect the cyber environment and organization and users' assets from threats and cybercrimes.[18]

The DICT launched the first NCSP in 2017, to cover the period 2017-2022. The NCSP 2022 defines cybersecurity as "the protection of information systems [...], the data within these systems, and the services that are provided by these systems from any unauthorized access, harm or misuse, whether it includes intentional or accidental, or from natural disasters."[19] This follows the definition of cybersecurity as the "preservation of confidentiality, integrity, and availability of information in the Cyberspace" used both by the ISO and the ITU. As stated in the previous section, this approach has long been criticized by civil society groups for being focused on the security of systems over the security of persons.

V. Digital Threats to Civic Space in the Philippines

The Freedom on the Net Report, an annual assessment of individual countries' internet freedom published by Freedom House, gave the Philippines a score of 65/100 in 2022, deeming it "partly free."[20] The last time the Philippines was marked "free" was in 2017, when it scored 72/100.[21] The country's performance went on a downward spiral since, scoring 69/100 in 2018, 66/100 in 2019, and 64/100 in 2020. The annual report is based on combined scores in three areas: Obstacles to Access, Limits on Content, and Violations of User Rights. Similar to Freedom House's framework, this paper zeroes in on three of the most pressing threats to civic space in the Philippines, particularly with regard to the use of technologies for surveillance, censorship, and disinformation.

A. Surveillance

Surveillance, especially as it relates to civic space, can generally be divided into two categories: mass surveillance and targeted surveillance. While we use the general term "surveillance" in this section, we refer largely to the mass surveillance architecture built by the Philippine government that is designed to cover the entire population. Here we refer to the kind of surveillance defined by Privacy International as that which involves "the acquisition, processing, generation, analysis, use, retention or storage of information about large numbers of people, without any regard to whether they are suspected of wrongdoing.[22]

18 Republic Act No. 10175, An Act Defining Cybercrime Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes.

19 National Cybersecurity Plan 2022," Department of Information and Communications Technology, May 2, 2017, https://dict.gov.ph/national-cybersecurity-plan-2022/

20 "Freedom on the Net 2022: Philippines," Freedom House, https://freedomhouse.org/country/philippines/freedom-net/2022

21 "Freedom on the Net 2017: Philippines," Freedom House, https://freedomhouse.org/country/philippines/freedom-net/2017

22 "Mass Surveillance," Privacy International, https://privacyinternational.org/learn/mass-surveillance

Instances of targeted surveillance that leads to the arrest and/or killing of journalists and activists will be covered in the next section on censorship.

1. The Philippine Surveillance Architecture

We begin by looking at the framework that allows the conduct of surveillance under Philippine law. Generally, the right against unlawful surveillance is protected by Article III Sections 2 and 3 of the Philippine Constitution.[23] There are, however, specific cases where communications surveillance is allowed by law, subject to certain conditions and processes. The Anti-Wiretapping Act, passed almost six decades ago in 1965, prohibits the covert interception or recording of any private communication or spoken word of another person or persons without the authorization of all parties to the communication. The law carves out an exception for law enforcement in specific instances such as in cases involving treason, espionage, provoking war and disloyalty in case of war, inciting to rebellion, sedition, and kidnapping, among others.

The Cybercrime Prevention Act of 2012 originally provided authority for law enforcement to conduct real-time collection of traffic data, but the provision was declared unconstitutional by the Supreme Court for giving law enforcement surveillance powers that are "too sweeping and lack restraint."[24] A bill filed by Senator Imee Marcos, a sister of President Ferdinand Marcos Jr., in the 18th Congress aimed to reinstate this section in the cybercrime law, arguing that there is "a dire need to put order to the tremendous activities in cyberspace for public good."[25]

During the Duterte administration, what used to be a very small and specific niche of exemptions where surveillance may be authorized, was expanded through the Anti-Terrorism Act (ATA) of 2020. The ATA repealed the previous Human Security Act and carved out certain instances where surveillance may be done on judicially declared or suspected terrorists as defined by the same law. With the new surveillance powers granted by this law, the importation of surveillance technology, the creation of a massive database through the recently launched Philippine Identification System (PhilSys), and a highly militarized cybersecurity architecture, it is clear that the Duterte government had an agenda to build a surveillance state.

Indeed, cyber securitization is closely connected with securitization in the guise of other concepts such as counterterrorism, counterinsurgency, and Duterte's War on Drugs. Notable in the National Cybersecurity Plan is the message from former Assistant Secretary for Cybersecurity and Enabling Technologies of the Department of ICT, Allan Cabanlong, which points to "policing the cyberspace" as necessary to protect Filipinos from "certain groups whose ideology is to destroy the order of our nation and are now using advanced and sophisticated technologies to carry out their plans." In his own message, former National Security Adviser Hermogenes C. Esperon Jr. said that cybersecurity is an important part of national security.

23 Article III, Sec. 2. states that "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable [;]" whereas Sec. 3 provides that "(1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law [.]".

24 G.R. No. 203335, Disini v. Secretary of Justice.

25 Senate Bill No. 1905, "An Act Amending Republic Act No. 10175 Otherwise Known as the "Cybercrime Prevention Act of 2012, and For Other Purposes".

It is noteworthy that among many instances of harassment and killing of journalists and activists, there were reported accounts of the victims being surveilled or followed by suspicious actors before the attacks. Zara Alvarez, an activist,[26] and Dr. Mary Rose Sancelan, a municipal health officer, [27] who were both red-tagged as alleged terrorists, both reported being tailed and threatened through SMS before they were slain on separate occasions during the pandemic. In July 2022, a military officer was caught conducting surveillance by taking photos and recording conversations during the wake of a former journalist and activist who was among those killed in a clash with the military.[28]

These point back to the argument that the right to privacy is inseparable from the freedoms of speech, association, and assembly. Surveillance and other forms of privacy violations are usually a precursor to other human rights violations, especially for targeted groups such as activists and journalists.

The right to privacy is inseparable from the freedoms of speech, association, and assembly. Surveillance and other forms of privacy violations are usually a precursor to other human rights violations, especially for targeted groups such as activists and journalists.

2. Surveillance Actors

Mapping the surveillance infrastructure in the Philippines is an arduous task, mainly because of the opaque and confidential nature of State surveillance. Based on their legal mandates, the following are the intelligence and security agencies that may be engaged in surveillance activities:[29]

1. National Security Council
2. Office of the National Security Adviser
3. National Intelligence Coordinating Agency
4. National Intelligence Committee
5. National Intelligence Board
6. Philippines
7. Directorate for Intelligence, Philippine National Police
8. Police Intelligence Group, Philippine National Police
9. Anti-Cybercrime Group, Philippine National Police
10. Office of the Deputy Director for Intelligence Services, National Bureau of Investigation
11. Cyber Crime Division, National Bureau of Investigation

26 Lian Buan, "Zara Alvarez asked for protection, but she died before the court could give it," *Rappler*, August 20, 2020, https://www.rappler.com/nation/zara-alvarez-petition-writ-amparo-habeas-data-court/

27 Catherine Gonzales, "Murder of Red-tagged doctor, husband could be related to work, NPA – police," *Inquirer.net*, December 21, 2020, https://newsinfo.inquirer.net/1374430/murder-of-red-tagged-doctor-husband-could-be-related-to-work-npa-police

28 John Sitchon, "What we know so far: Nikka dela Cruz, the Cebuana killed in Negros Occidental encounter," *Rappler*, July 20, 2022, https://www.rappler.com/nation/visayas/what-we-know-so-far-nikka-dela-cruz-cebuana-killed-negros-occidental-encounter/

29 State of Privacy Philippines," Privacy International, January 26, 2019 https://privacyinternational.org/state-privacy/1009/state-privacy-philippines

Under the Anti-Terrorism Act of 2020, law enforcement agents or military personnel may, upon a written order of the Court of Appeals, conduct communications surveillance (a) between members of a judicially declared and outlawed terrorist organization; (b) between members of a designated person; or (c) any person charged with or suspected of committing any of the crimes defined and penalized under the same law. Other special laws that allow the conduct of surveillance by law enforcement include the Expanded Anti-Trafficking in Persons Act and the Anti-Child Pornography Act.

3. Use of Technology for State Surveillance

A 2015 report by the Foundation for Media Alternatives outlined some of the surveillance technologies that were reported to have been acquired by the Philippine government. The report shows that over the years, the Philippine government had acquired or, at the very least, expressed an intention to acquire, technologies such as a border control software that may be used to quickly retrieve information on persons who may be trying to leave the country after committing a crime, a social media intelligence solution, an intrusion technology that allows its operator to bypass any encryption technology installed on a device, and radio frequency test equipment.[30]

Acquisition of surveillance technologies continued during the Duterte administration, where about PhP10 million worth of spyware was reported to have been acquired from the British government. According to reports, the sale included International Mobile Subscriber Identity (IMSI) catchers, which are used to eavesdrop on telephone conversations, as well as tools to monitor internet activity.[31] This was especially alarming given Duterte's history of using surveillance mechanisms for his drug war even when he was still the mayor of Davao City.[32]

Several surveillance technologies were acquired and used during the COVID-19 pandemic, most of which were justified by the government with the need to monitor public places for quarantine monitoring.[33] These include the installation of surveillance camera networks, some equipped with artificial intelligence technology to detect real-time movement of residents,[34] and the deployment of camera drones by police to detect quarantine violations.[35] Not much is known about when these COVID-specific technologies will cease to be used, making them susceptible to misuse as tools for the unlawful monitoring of vulnerable groups and ordinary citizens.

30 Foundation for Media Alternatives, "TIKTIK: An Overview of the Philippine Surveillance Landscape," September 2015, https://www.fma.ph/wp-content/uploads/2017/10/Briefing-Paper-1-DRAFT-1.pdf

31 Hannah Ellis-Petersen, "Britain sold spying gear to Philippines despite Duterte's brutal drugs war," *The Guardian*, February 21, 2018, https://www.theguardian.com/world/2018/feb/21/britain-sold-spying-gear-to-philippines-despite-dutertes-brutal-drugs-war

32 George Joseph, "Inside the Video Surveillance Program IBM Built for Philippine Strongman Rodrigo Duterte," *The Intercept*, March 20, 2019, https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/

33 Foundation for Media Alternatives, "A Pandemic as Vector for State Surveillance and Other Abuses," September 2021, https://fma.ph/2021/09/13/a-pandemic-as-vector-for-state-surveillance-and-other-abuses/

34 "Pasig village boosts measures to mitigate spread of Covid-19," *Philippine News Agency*, March 30, 2020, https://www.pna.gov.ph/articles/1098189

35 Christia Marie Ramos, "11 drones now in Cebu City to monitor quarantine compliance – Eleazar," *Inquirer.net*, June 28, 2020, https://newsinfo.inquirer.net/1298698/11-drones-now-in-cebu-city-to-monitor-quarantine-compliance-eleazar

4. Surveillance through "Smart Cities"

The policing of physical spaces through the use of technology was a recurring theme throughout the Duterte administration. This is most evident in the multitude of "smart city" or "safe city" projects that cropped up during this period. One such initiative is Safe Philippines, a surveillance system project that aims to install high-definition and advanced CCTV cameras in selected cities in Metro Manila to supposedly curb crime and improve emergency response time. Majority of the P20.31Billion project is funded through a soft loan from China Eximbank, and the contractor is the China International Telecommunication Construction Corporation, with some equipment provided by Huawei, another China-based tech giant.[36] This, despite allegations of espionage against Huawei that caused it to be banned in several countries, and evidence of the company's involvement in domestic surveillance activities in China.[37] This is not Huawei's first foray into a safe city initiative in the Philippines. The company previously piloted its Safe City project in Bonifacio Global City. This involved the installation of high-definition surveillance cameras connected to a command center through wi-fi. The technology was supposedly able to "detect crime and criminal intrusions."[38]

The branding of "safe cities" fits well within Duterte's anti-crime rhetoric, which he seemed to have already figured out years before he was elected President. In 2012, IBM announced the establishment of an Intelligent Operations Center (IOC) in partnership with the Davao City government, which was then headed by Rodrigo Duterte's daughter, Sara who is now vice-president of the country. The IOC became operational in 2013, just in time for the father's return to the mayoral seat.[39] In an interview with *The Intercept*, a former sales officer who worked with the project to improve Davao's Public Safety and Security Command Center revealed that the technology deployed under the project was "probably the first-ever video analytics surveillance that was done in Asia."[40] These multiple projects by Huawei and IBM demonstrate how easy it is for foreign companies to import surveillance technologies into the Philippines, and they don't even need to call it surveillance. They only need to call it a "smart city" or "safe city" project and it will fly under the radar, lumped with the plethora of other initiatives posing as part of the country's digital transformation."

36 Loreben Tuquero, "Año says China-funded Safe Philippines project will be 'all-Filipino'," *Rappler*, November 22, 2019, https://www.rappler.com/nation/245529-ano-china-funded-safe-philippines-project-all-filipino/

37 Eva Dou, "Documents link Huawei to China's surveillance programs," *The Washington Post*, December 14, 2021, https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/

38 "Transforming Bonifacio Global City into a Safe City with Huawei," Huawei, https://e.huawei.com/topic/leading-new-ict-ua/safe-city-case.html

39 George Joseph, "Inside the Surveillance Program IBM Built for Rodrigo Duterte," *The Intercept*, March 20, 2019, https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/

40 Ibid.

This reflects the creeping global concern over China's exportation of surveillance technology through smart cities.[41] It's worth noting, however, that China is not the only state that exports surveillance technology. Leaked documents show that past administrations were in talks with several surveillance equipment manufacturers for technologies such as border control and monitoring software, social media intelligence, and intrusion technology that can collect data from a device undetected.[42]

5. Surveillance through Digital Identity and Profiling

A more seemingly innocuous threat than blatant surveillance is profiling through digital identity. As noted in the Funders Initiative for Civil Society (FICS) report on the global counter-terrorism agenda and civic space,[43] there is an increasing convergence of digital identity systems, which usually include biometric data, and the push for financial inclusion. This has created an "unprecedented global drive for high-tech national ID systems" that come with massive risks of abuse by oppressive actors to conduct mass or targeted surveillance and harassment of activists and other vulnerable groups. In the Philippines, this comes in the form of PhilSys, or the Philippine Identification System, a national ID system created in 2018 after decades of attempts and failures by both the legislative and executive branches.

Like most national ID systems all over the world, the PhilSys has been closely backed by the World Bank since its development phase until its implementation at the time of writing.[44] This support includes both technical and financial assistance, with a $600 million loan to support the PhilSys' rollout.[45] And like the smart city projects, this national ID agenda is usually lumped under the broad goal of "digital transformation".

But the Philippine government's obsession with identity systems and massive identity databases does not stop with the PhilSys. Local governments have been establishing their own localized ID systems. These local ID systems became even more popular during the pandemic, as they were meant to facilitate distribution of financial aid and other government services as part of COVID response. Contact tracing systems that were established during the pandemic became sources for massive databases as well, most of which were created and held separately (i.e., not in a unified national database) by local governments or private contractors.

41 James Kynge, et al., "Exporting Chinese surveillance: the security risks of 'smart cities'," *Financial Times*, June 9, 2021, https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab

42 Foundation for Media Alternatives, "TIKTIK: An Overview of the Philippine Surveillance Landscape," September 2015, https://www.fma.ph/wp-content/uploads/2017/10/Briefing-Paper-1-DRAFT-1.pdf

43 Dr Gavin Sullivan and Chris Jones, "Is the global counter-terrorism agenda shrinking civic space?," Funders Initiative for Civil Society, May 2022, https://www.fundersinitiativeforcivilsociety.org/wp-content/uploads/2022/05/Is-CT-shrinking-civic-space-FICS-May-2022.pdf

44 Center for Human Rights & Global Justice, "Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID," June 2022, https://chrgj.org/wp-content/uploads/2022/06/Report_Paving-a-Digital-Road-to-Hell.pdf

45 Beatrice Laforga, "World Bank approves $600-million loan for PHL 4Ps program," *Business World*, September 30, 2020, https://www.bworldonline.com/economy/2020/09/30/320062/world-bank-approves-600-million-loan-for-phl-4ps-program/

Having surprisingly eluded both congressional and presidential approval for decades, the SIM card registration law seems to be the last piece of the puzzle, the last tool needed to complete the government's surveillance arsenal. The last version of the bill that almost passed in 2022 just before the end of Duterte's term, was especially reflective of this vision. The bill proposed that apart from requiring the registration of all SIM cards, all social media account providers shall require the real names and phone numbers of users to be registered upon account creation. According to the version of the bill passed by both houses of Congress, this is to "deter the proliferation of SIM card, internet or electronic communication-aided crimes, such as, but not limited to: *terrorism*; text scams; unsolicited, indecent or obscene messages; bank fraud; libel; anonymous online defamation; trolling; hate speech, and *the spread of digital disinformation or fake news as defined under pertinent laws*. (Emphasis supplied)" The inclusion of terrorism and disinformation in the bill demonstrates how surveillance measures – or at least, attempts to expand the surveillance powers of government – are intricately linked with the other threats to civic space described in this paper.

The use of surveillance measures – in this case, a massive database of citizen data – to supposedly address a sweeping list of crimes, is against the principles of necessity and proportionality as envisioned in the International Principles on the Application of Human Rights Law to Communications Surveillance.[46] Furthermore, the erosion of anonymity offered by mandatory identity registration, especially in social media, is disproportionately dangerous for women and the LGBTQ community, whose self-expression is usually tied to their lived identities rather than their legally recognized ones.

"Function creep" is a major concern in most ID systems, including national ID systems, mandatory SIM card registries, and contact tracing systems. It refers to the phenomenon where information collected for one specified purpose tends to be used for ever-expanding and undisclosed purposes.[47] The narratives used by proponents in government to defend the PhilSys and SIM card registration point to the risk of function creep. The PhilSys alone is a favorite talking point of government officials when speaking about almost any issue. It has been named as a possible tool for aid distribution during the pandemic by the Department of Social Welfare and Development,[48] for vaccine distribution by the National Economic Development Authority,[49] and, unsurprisingly, for law enforcement by the Philippine National Police.[50]

46 Electronic Frontier Foundation and Article 19, "Necessary & Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance," May 2014, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf

47 Evelina Manukyan and Joseph Guzzetta, "How function creep may cripple app-based contact tracing," International Association of Privacy Professionals, May 27, 2020, https://iapp.org/news/a/how-function-creep-may-cripple-app-based-contact-tracing/

48 Christine Cudis, "Nat'l ID system to help ease delivery of social services: DSWD," *Philippine News Agency*, June 11, 2020, https://www.pna.gov.ph/articles/1105656

49 Ted Cordero, "NEDA offers use of nat'l ID for COVID-19 vaccine distribution," *GMA News Online*, December 16, 2020, https://www.gmanetwork.com/news/topstories/nation/768208/neda-offers-use-of-nat-l-id-for-covid-19-vaccine-distribution/story/

50 Benjamin Pulta, "PNP eyes linking police database to nat'l ID system," Philippine News Agency, August 7, 2018, https://www.pna.gov.ph/articles/1043966

Source: Photo by Raffy Lerma
Employees, journalists, celebrities, and supporters of media network ABS-CBN show their dissent a week after Congress rejected their franchise renewal with a noise barrage and motorcade outside the ABS-CBN compound in Quezon City on July 18, 2020.

This narrative of the PhilSys as a magic pill for every ill of Philippine society is likely to continue during Marcos Jr.'s presidency. In his first month as president, Marcos Jr. temporarily assumed leadership of the Department of Agriculture. When asked about immediate measures to assist sectors affected by the food crisis, Marcos was quick to point to the issuance of national IDs to facilitate aid distribution, saying that "[it] all really depends on everyone having their national ID. It's a good database that the government should have."[51]

B. Censorship

1. Censorship through Libel and Attacks on Freedom of the Press

A unique feature of the Philippines' Cybercrime Prevention Act (CPA) is that it includes the crime of cyberlibel, which is not included in the Budapest Convention, from which the CPA was supposedly patterned. This, despite the fact that Filipino journalists and activists have long been calling for the decriminalization of (traditional) libel under the Revised Penal Code. The cyberlibel provision was a last-minute insertion by Senator Vicente Sotto III following a spate of criticism hurled against him in social media earlier that year. Sotto, of course, vehemently denied this.[52]

51 "Marcos To Head DA 'For Now'," *Page One.PH*, June 21, 2022, https://pageone.ph/marcos-to-head-da-for-now/

52 Norman Bordadora, "Sotto admits he proposed online libel provision," *Inquirer.net*, October 2, 2012, https://technology.inquirer.net/17718/sotto-admits-he-proposed-online-libel-provision

Today, cyberlibel has become the weapon of choice by politicians and celebrities against their critics and opponents. It was also a critical weapon of the Duterte regime against a free and independent press, as evidenced by the stack of cyberlibel cases (and convictions) against the news organization Rappler and its reporters, along with other means of regulatory harassment.

The first round of harassment against *Rappler* came in December 2016, just a few months into the Duterte regime, when the Office of the Solicitor General (OSG) requested the Philippines' Securities and Exchange Commission (SEC) to investigate the news platform's issuance of PDRs (Philippine Depositary Receipts) to foreign investors. The OSG alleged that this was in contravention of the constitutional restriction against foreign ownership of Philippine media. The case eventually resulted in the revocation of *Rappler's* license to operate in 2018. After a few more years of litigation, the SEC in June 2022 affirmed its decision to revoke *Rappler's* certificate of incorporation, effectively "confirm[ing] the shutdown of *Rappler*."[53]

Cyberlibel ... was also a critical weapon of the Duterte regime against a free and independent press, as evidenced by the stack of cyberlibel cases (and convictions) against the news organization Rappler and its reporters, along with other means of regulatory harassment.

Meanwhile, in October 2017, the first of a long series of cyberlibel cases was filed against *Rappler's* CEO and founder Maria Ressa and Reynaldo Santos, Jr. a former *Rappler* researcher, over an article originally published in May 2012, four months before the enactment of the Cybercrime Prevention Act. While the complaint was initially junked for being past the prescriptive period, the dismissal was eventually reversed and a warrant of arrest was served.[54] After more than a year of trial and legal proceedings, the Manila Regional Trial Court found Ressa and Santos guilty of cyberlibel. The Court of Appeals upheld this conviction, ruling that the prescriptive period of cyberlibel is 15 years, compared to ordinary libel that prescribes in only one year.[55] This is a dangerous precedent that makes cyberlibel an even more powerful weapon in the harassment of journalists and even ordinary citizens.

53 "TIMELINE: Rappler-SEC case," *CNN Philippines*, June 30, 2022, https://www.cnnphilippines.com/news/2022/6/30/Rappler-SEC-case-timeline.html

54 TIMELINE: Rappler's cyberlibel case," *Rappler*, February 14, 2019, https://www.rappler.com/newsbreak/iq/223460-timeline-cyber-libel-case/

55 Lian Buan, "When CA upheld Rossa's conviction, it extended cyberlibel shelf to 15 years," *Rappler*, July 12, 2022, https://www.rappler.com/nation/when-court-appeals-upheld-maria-ressa-conviction-made-cyber-libel-shelf-life-longer/

The cyberlibel cases against Rappler were just the beginning of a long line of cases against journalists and citizens who expressed their discontent with the Philippine government during the Duterte and early Marcos Jr. administrations. In fact, official figures from the Department of Justice Office of Cybercrime reveal that 30% of cyber cases filed (1,131 of 3,770 cases) have been dismissed. Of the 3,770 cases of cyberlibel filed, there have been 12 convictions and four acquittals. Three of these convictions are of journalists, including Maria Ressa. Meanwhile, data from the Philippine National Police shows that cyberlibel cases make up 20% of all cybercrimes they investigate.[56]

In August 2022, well-known activist and academic Walden Bello was arrested on charges of libel by a former information officer for the then-newly elected Vice President Sara Duterte. The complaint stemmed from a Facebook post by Bello alleging that Duterte's former employee was involved in illegal drugs after a party that he attended was raided by the police for drugs.[57] As highlighted in the boxed section below, the weaponization of libel and cyberlibel against government critics became more prominent during the COVID-19 crisis under the guise of the government's campaign against COVID-related disinformation.

Parallel to this barrage of libel cases, a key tactic in censorship during Duterte's term was the targeted harassment of established news outfits and the erosion of trust in the media as a whole. From a legal and regulatory standpoint, there isn't much room for prior restraint in the Philippines. But with what limited toolbox was available, government forces were able to wield political power against the free press. In a government-mandated shutdown, as publicly admitted by Duterte himself right before his term ended,[58] what used to be one of the longest running and major broadcast networks in the country went permanently off-the-air in 2020 for the technical reason that its congressional franchise had expired and was not renewed.

The removal of ABS-CBN and its regional channels from public television was a huge setback to the dissemination of critical information during the COVID-19 pandemic, especially for those living in far-flung areas and low-income households whose main source of information and entertainment were traditional radio and television channels like ABS-CBN.[59] This points to another fundamental right that is often overlooked in definitions and discussions of civic space – the right to access information. The ABS-CBN closure removed one of the biggest spaces for discursive practices in the country. The Center for Media Freedom and Responsibility (CMFR) highlighted that, especially during the pandemic, a giant nationwide network like ABS-CBN is valuable to "air timely warnings of imminent public danger, to disseminate crucial information in times of emergency, saving lives and mitigating the impact of calamity and disaster with appropriate assistance," as well as providing political information that fuels civic engagement and political participation.[60] This, along with the targeted harassment of *Rappler*, demonstrates the Duterte government's intention of dissolving platforms and quashing opportunities for critical discourse.

56 Lian Buan, "Decriminalize libel: PH junked one-third of cyberlibel cases filed since 2012," *Rappler*, July 20, 2022, https://www.rappler.com/newsbreak/in-depth/decriminalize-philippines-junked-cyber-libel-cases-since-2012/

57 Carlos H. Conde, "Philippine Activist Arrested for Cyber-libel," *Human Rights Watch*, August 9, 2022 https://www.hrw.org/news/2022/08/09/philippine-activist-arrested-cyber-libel

58 Mark Ernest Amratian, "Duterte admits using presidential powers to target ABS-CBN," *Yahoo News*, June 28, 2022, https://ph.news.yahoo.com/duterte-admits-using-presidential-powers-to-target-abs-cbn-032708317.html

59 Jason Gutierrez, "Duterte's Shutdown of TV Network Leaves Void Amid Coronavirus Crisis," *The New York Times*, May 14, 2020, https://www.nytimes.com/2020/05/14/world/asia/duterte-philippines-tv-network-ABS-CBN.html

60 Center for Media Freedom and Responsibility, "Closing down ABS-CBN and its impact on free speech in the Philippines," *IFEX*, May 7, 2020, https://ifex.org/closing-down-abs-cbn-and-its-impact-on-free-speech-in-the-philippines/

2. Censorship through Cyberattacks

As red-tagging from both government and non-government actors ramped up, distributed denial of service (DDoS) became a common attack tactic on progressive groups, particularly on alternative and independent media groups. DDoS attacks are not an uncommon form of cyber-attack, but what made them notable during the Duterte administration was their sheer frequency and scope, and the specific network of media organizations targeted across several instances. The first major attack happened in December 2018,[61] and another three-month long series of attacks was observed in December 2021.[62] A Facebook page called "Pinoy Vendetta" claimed that one of its members conducted the December 2021 attacks. Pinoy Vendetta had earlier been vocal in its support for the NTF-ELCAC and its "mission to bring down and end the CPP-NPA-NDF." The group was subsequently publicly endorsed by the NTF-ELCAC, with its spokesperson calling its members "computer geniuses."[63] Both attacks were investigated by the Swedish digital forensics non-profit Qurium Media Foundation, who assessed that although three separate media organizations were targeted in December 2021, similar attack signatures suggest that they were done by the same perpetrator.[64] Further, upon investigation of a series of DDoS attacks in 2021, some of the attacks were found to have originated from IP addresses that are linked to the Department of Science and Technology and the Philippine military.[65]

Qurium's investigation of the DDoS attacks on *Bulatlat*, an independent media outlet, in November 2021 showed that the attacks were coming from thousands of Facebook accounts. Further investigation showed that this was done through an elaborate operation where a Vietnamese troll farm used malicious links disguised as links to pornography to capture the credentials of Facebook users and redirect the traffic to *Bulatlat*. Qurium also found that this operation went largely undetected as the operators used a "bouncing domain" and "residential proxies" to circumvent Meta's mechanisms to detect phishing scams and malicious links.[66]

61 "Alternative media groups file civil case amid cyberattacks," *Rappler*, March 29, 2019, https://www.rappler.com/technology/226968-alternative-media-groups-file-civil-case-cyberattacks-march-2019/

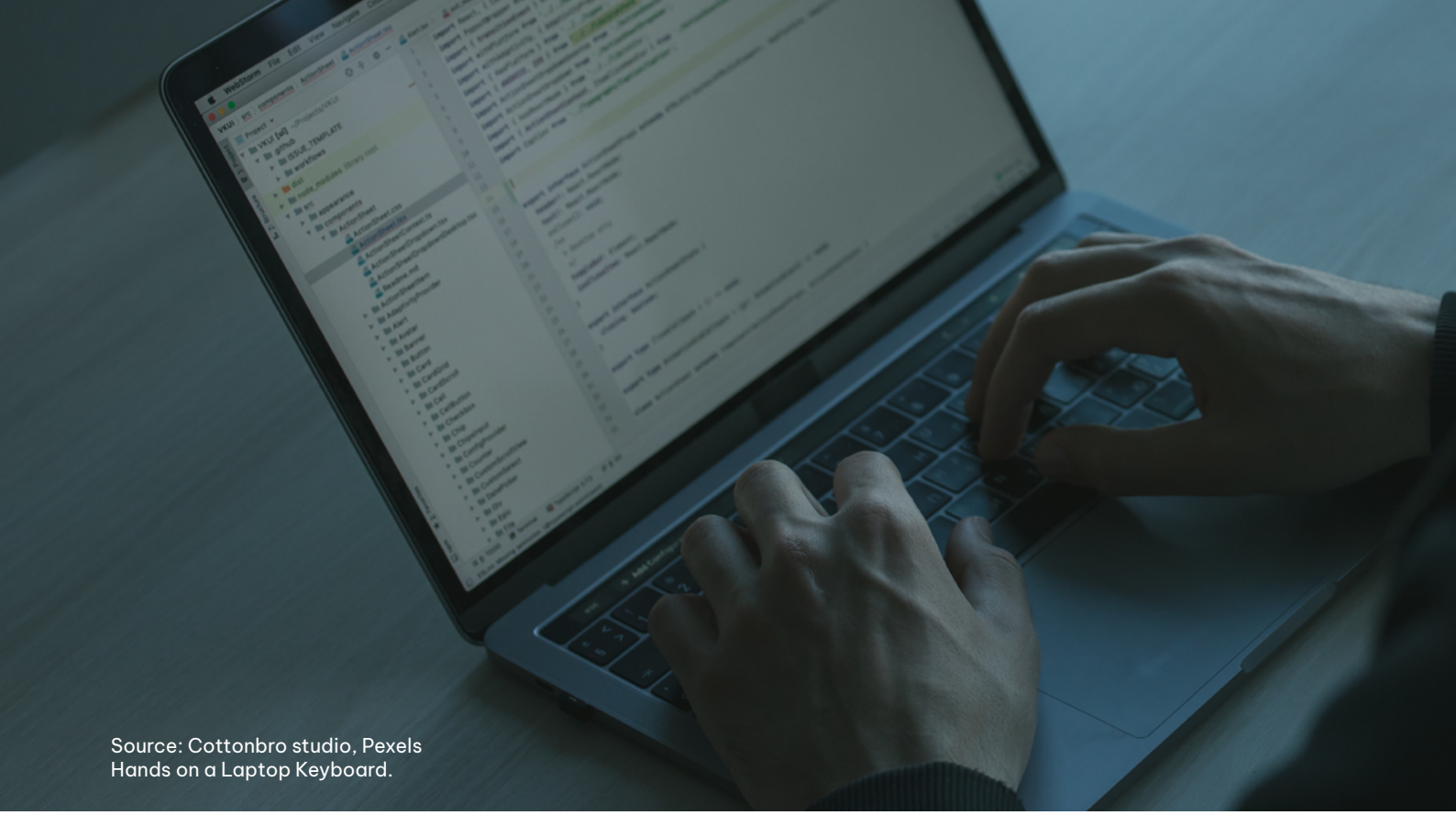
62 Alyssa Mae Clarins, "Cyberattacks traced to PH hackers hailed by gov't as 'computer geniuses,' probe shows," *Altermidya*, March 15, 2022, https://www.altermidya.net/cyberattacks-traced-to-ph-hackers-hailed-by-govt-as-computer-geniuses-probe-shows/

63 Galo Gonzales, "Hacker group mounts DDoS attacks vs PH news outlets, hailed by gov't," *Rappler*, February 24, 2022, https://www.rappler.com/technology/ntf-elcac-ddos-attacks-endorsement/

64 Alyssa Mae Clarine, "Cyberattacks traced to PH hackers hailed by gov't as 'computer geniuses,' probe shows," *Altermidya*, March 15, 2022, https://www.altermidya.net/cyberattacks-traced-to-ph-hackers-hailed-by-govt-as-computer-geniuses-probe-shows/

65 Gelu Gonzales, "Military, DOST links found in DDoS attacks on media – report," *Rappler*, June 23, 2021, https://www.rappler.com/technology/qurium-links-dost-military-found-ddos-attacks-altermidya-bulatlat/

66 Vittoria Elliott, "A Sprawling Bot Network Used Fake Porn to Fool Facebook," *Wired*, September 26, 2022, https://www.wired.com/story/facebook-bots-ddos-attack/



Source: Cottonbro studio, Pexels
Hands on a Laptop Keyboard.

Red-tagging and attacks on journalists – especially those from independent media groups – have continued through the Marcos Jr. administration. In June 2022, the National Telecommunications Commission ordered the blocking of 26 websites, alleging that the websites are "affiliated to and are supporting terrorists and terrorist organizations" designated as such by several resolutions of the Anti-Terrorism Council. The blocked websites included those of independent media groups, such as *Bulatlat* and *Pinoy Weekly*, as well as those of the Save Our Schools Network of NGOs advocating for the right to education, and the Rural Missionaries of the Philippines, a group of priests, nuns, and laypeople.[67]

3. Censorship through Content Moderation

Social media platforms, each with their own legal terms and policies, are another battleground when it comes to regulation of speech, which comes in the form of content moderation. Over the years, social media content moderation has been the subject of too many controversies – from the use of machine learning to make takedown decisions,[68] to labor issues involving third-party content moderators mostly from countries like the Philippines.[69] But for this paper, it is crucial that we look at the content policies of social media platforms – particularly Facebook – as it will give us a good idea of how the concepts of "safety" and "security" are operationalized in the digital spaces that host a significant chunk of Filipinos' lives.

67 Raymond Carl Dela Cruz, "NTC orders ISPs to block terror group-related sites," *Philippine News Agency*, June 22, 2022, https://www.pna.gov.ph/articles/1177276

68 Span dāna Singh, "Everything in Moderation: An Analysis of How Internet Platforms Are Using Artificial Intelligence to Moderate User-Generated Content," *New America*, July 22, 2019, https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/case-study-facebook/

69 Vittoria Elliott and Devendra Pamar, "The despair and darkness of people will get to you," *Rest of World*, July 22, 2020, https://restofworld.org/2020/facebook-international-content-moderators/

In the general section of Facebook's Community Standards, it defines safety as "[removing] content that could contribute to a risk of harm to the physical security of persons" as well as content that "threatens people [and] has the potential to intimidate, exclude or silence others."[70] Its specific definitions of terms such as hate speech and terrorism, however, leave much to be desired.[71] Despite these policies, Facebook remains a breeding ground for all forms of harassment, including gender-based harassment and violence, that have been shown to have a chilling effect on the online speech of women and other vulnerable groups, and democratic discourse as a whole.[72] Figures about online gender-based violence in the Philippines show Facebook as the top platform where various forms of online gender-based violence were perpetrated during the pandemic.[73] The fact is that although Meta supposedly has local policy offices, the directives and key decisions still come from its American headquarters, and therefore reflect the largely white, male, and libertarian corporate ethos of the company.[74]

Given Facebook's massive user base in the Philippines, the lack of involvement of Filipino stakeholders in its decision making deserves to be questioned. It is also important to investigate and question the involvement of Facebook and other foreign technology companies in providing internet access to Filipinos. Ultimately, the issue of net neutrality – which is the principle that internet service providers (ISPs) should treat all data that travels over their networks fairly and without discrimination in favor of particular apps, websites, or services[75] – is an issue of censorship and the right of people to access information necessary to participate in civic space freely and meaningfully.

C. Disinformation and Securitized Responses

Rodrigo Duterte became the 16th President of the Philippines on June 30, 2016. Duterte's campaign and eventual success was a turning point in Philippine history due to his team's use of digital tactics on social media platforms. Trolls and volunteers were hired to bolster support for his election in which they would spread information to promote and defend him against critics.[76]

70 "Facebook Community Standards," Meta Transparency Center, https://transparency.fb.com/policies/community-standards

71 Article 19, "Facebook Community Standards: Analysis against international standards on freedom of expression," July 30, 2018, https://www.article19.org/resources/facebook-community-standards-analysis-against-international-standards-on-freedom-of-expression/

72 Duna Mijatović, "No space for violence against women and girls in the digital world," Council of Europe Commissioner for Human Rights, March 15, 2022, https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

73 Foundation for Media Alternatives, "Submission on domestic violence in the context of COVID 19 to the United Nations Special Rapporteur on violence against women, its causes and consequences," June 30, 2020,

74 Ysabel Gerard, "Social media content moderation: six opportunities for feminist intervention," *Feminist Media Studies 20*, no. 5 (June 2020): 748-751, https://doi.org/10.1080/14680777.2020.1783807

75 "Net Neutrality," Electronic Frontier Foundation, https://www.eff.org/issues/net-neutrality

76 Pia Ranada, "Duterte says online defenders, trolls hired only during campaign," *Rappler*, July 25, 2017, https://www.rappler.com/nation/176615-duterte-online-defenders-trolls-hired-campaign/

The disinformation-marred campaign and election period made the Philippines known as "Patient Zero," the first nation where an election is shown to be heavily influenced by disinformation on online platforms.[77] Coordinated disinformation and online propaganda continued throughout Duterte's six-year term, which was also marked by human rights violations. Various digital tactics were used to attack critics of Duterte and his administration. Independent media, opposition politicians, and fact-checking organizations were targeted while disinformation and misinformation that espoused Duterte's authoritarian rhetoric were allowed and even encouraged to spread in online and offline channels.[78] Troll armies were also employed during the COVID pandemic to defend the Philippine government's COVID response and drown out criticism.[79]

The meteoric rise of disinformation and propaganda online was further bolstered by the erosion of public trust in traditional media as the fourth estate. In fact, according to research by the Reuters Institute for the Study of Journalism, social media is now the biggest source of news by Filipinos (72%), overshadowing traditional platforms like television (61%) and print (16%). Among social media and messaging platforms, Facebook, YouTube, and Facebook Messenger rank as the biggest sources of news.[80]

A study on digital disinformation during the 2019 midterm elections noted that micro-media manipulation, which refers to micro-targeting seeded specific political propaganda at discrete groups, had become a new insidious strategy to disseminate propaganda while evading fact checkers and content moderators.[81] This means that disinformation now thrives at the level of small communities and private groups. This trend is noteworthy because while Facebook can penalize accounts and pages for hate speech or inauthentic coordinated behavior, it is unable to do the same for closed groups and communities because of privacy protections. The only actors who can take down or control the content in a closed group are its administrators or moderators. As the report notes, closed groups often operate as echo chambers or filter bubbles that communities of the same inclinations, whether political or otherwise, go to in order to affirm each other's beliefs.

Indeed, the rise of disinformation in social media also highlights the closing of digital spaces for discourse through the fragmentation of the internet and platforms that encourage the creation and sustenance of echo chambers. The 2022 Freedom on the Net report speaks of a global trend of authoritarian governments pushing to "divide the open internet into a patchwork of repressive enclaves" by blocking foreign websites, hoarding personal data, and centralizing their technical infrastructures under an internet governance model that promotes "cyber sovereignty."[82]

77 Ronald Mendoza, Imelda Danila, and Jurel Yap, "Philippines: diagnosing the infodemic," *The Interpreter*, December 1, 2021, https://www.lowyinstitute.org/the-interpreter/philippines-diagnosing-infodemic

78 Samantha Bradshaw and Philip Howard, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation," *Oxford Internet Institute*, July 17, 2017, https://demtech.oii.ox.ac.uk/research/posts/troops-trolls-and-troublemakers-a-global-inventory-of-organized-social-media-manipulation/

79 Lynzy Billing, "Duterte's troll armies drown out Covid-19 dissent in the Philippines," *Coda Story*, July 21, 2020, https://www.codastory.com/disinformation/philippines-troll-armies/

80 Yvonne Chua, "Digital News Report: Philippines," *Reuters Institute for the Study of Journalism*, June 23, 2021, https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2021/philippines

81 Jonathan Corpus Ong, Ross Tapsell, and Nicole Curato, "Tracking Digital Disinformation in the 2019 Philippine Midterm Election," *New Mandala*, August 2019, https://www.newmandala.org/wp-content/uploads/2019/08/Digital-Disinformation-2019-Midterms.pdf

82 Adrian Shahbaz, Allie Funk, and Kian Vesteinsson, "Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet," *Freedom House*, https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

The Philippines is believed to be Patient Zero in the global disinformation crisis, but equally or perhaps even more alarming are the solutions proposed to address it. Just within Duterte's term, several bills were filed to counter "fake news" with the proposed measures ranging from mere fact-checking to the regulation of and imposition of penalties on social media companies, to mandatory registration of social media accounts in a government-held database.

Securitized responses look at disinformation, hate speech, targeted harassment, and even gender-based violence as one massive, homogenous security threat – which they're not – and the proposed solutions are not at all nuanced. The perfect illustration of this is the country's cybercrime law, which looks at all offenses done through the use of ICTs on the same level. Apart from cyberlibel, Section 6 of the cybercrime law, which categorizes as cybercrime all crimes covered by the Revised Penal Code and by special laws when committed with the use of ICTs, has also been used to increase penalties for online speech purported to be disinformation.

This tendency of the government to impose a securitized response to disinformation is not unique to the Philippines. The Freedom Online Coalition, in its submission to the Office of the United Nations High Commissioner for Human Rights regarding the practical application of the UN Guiding Principles on Business and Human Rights in the global technology sector, warns against the tendency of governments to "unduly restrict, moderate, or manipulate online content or disrupt networks to deny users access to information, contrary to their international obligations and often under vague justifications of 'security', 'public order', or the false pretention of combating 'fake news'."[83]

It is highly ironic that the Philippines appears to foreign actors as a fertile testing ground for disinformation tactics because of its "relatively underdeveloped regulatory infrastructure,"[84] because technically speaking, there *are* regulatory structures in place that are supposed to counter such activities. Unlike most of its Asian neighbors, the Philippines has had both data protection and competition laws in place since 2012 and 2014, respectively. It has a functioning National Privacy Commission and a Philippine Competition Commission that each have the power to hold social media companies accountable to the Filipino people. Yet neither of these government agencies has made a significant effort to penalize or even investigate mammoth platforms such as Facebook for the harms their technologies have facilitated and their undue influence on Philippine democracy.

83 The Freedom Online Coalition's submission to the OHCHR regarding the practical application of the UNGPs in the global technology sector (A/HRC/RES/47/23)," Office of the United Nations High Commissioner for Human Rights, March 11, 2022, https://www.ohchr.org/sites/default/files/2022-03/Freedom-Online-Coalition.pdf

84 Paige Occeñola, "Exclusive: PH was Cambridge Analytica's 'petri dish' – whistle-blower Christopher Wylie," *Rappler*, September 10, 2019, https://www.rappler.com/technology/social-media/239606-cambridge-analytica-philippines-online-propaganda-christopher-wylie/

VI. In Focus: Securitized COVID-19 Response with the use of ICTs

With most transactions and everyday activities including school and work moving online, so have most efforts to restrict civic space and human rights. In the case of the Philippines, the threats and attacks on civic space that we identified earlier (i.e., surveillance, censorship, and securitized disinformation response), were amplified during the COVID-19 pandemic.

As highlighted by another report in this series (See ***'Not Safe: Securitization of the COVID-19 Crisis and its Impact on Civic Space in the Philippines'*** *by Mary Jane N. Real*), the Duterte government's approach to the COVID-19 response was highly securitized and militarized, and key to this strategy was the implementation of various levels of "community quarantine" or lockdowns. Several technologies were employed for quarantine enforcement, including the installation of surveillance cameras, the use of artificial intelligence to monitor the movements of residents in high-risk areas in real time,[85] and the use of camera drones by the police to detect quarantine violations.[86] In September 2020, the government task force charged with implementing community quarantine protocols[87] directed the national police to monitor social media for accounts of quarantine violations.[88]

Complementing these surveillance measures were attempts of the government to control online speech, particularly social media content that are critical of the Philippine government's COVID-19 response.

The Bayanihan to Heal as One Act, the law that declared a national emergency arising from the COVID-19 pandemic, included a provision that penalizes COVID-related disinformation. The penalized acts were defined as follows:

> *(f) Individuals or groups creating, perpetrating, or spreading false information regarding the COVID-19 crisis on social media and other platforms, such information having no valid or beneficial effect on the population, and are clearly geared to promote chaos, panic, anarchy, fear, or confusion; and those participating in cyber incidents that make use or take advantage of the current crisis situation to prey on the public through scams, phishing, fraudulent emails, or other similar acts;*

Rights advocates vehemently opposed this particular provision, asserting that the language is vague enough to allow possible abuse and misuse by State actors and suppress free speech.[89]

Case study continued on next page >>>

85 Pasig village boosts measures to mitigate spread of Covid-19," *Philippine News Agency*, March 30, 2020, https://www.pna.gov.ph/articles/1098189

86 Christia Marie Ramos, "11 drones now in Cebu City to monitor quarantine compliance – Eleazar," *Inquirer.net*, June 28, 2020, https://newsinfo.inquirer.net/1298698/11-drones-now-in-cebu-city-to-monitor-quarantine-compliance-eleazar

87 The Joint Task Force COVID-19 Shield is composed of the Philippine National Police, the Armed Forces of the Philippines, the Philippine Coast Guard, and the Bureau of Fire Protection. It serves as the enforcement arm of the national government in implementing quarantine rules and protocols during the COVID-19 pandemic.

88 JC Gotinga, "Police to 'regularly monitor' social media for quarantine violations," *Rappler*, September 5, 2020, https://www.rappler.com/nation/police-regularly-monitor-social-media-quarantine-violations

89 Lian Buan, "Bayanihan Act's sanction vs 'false' info the 'most dangerous,'" *Rappler*, March 29, 2020, https://www.rappler.com/nation/256256-sanctions-fake-news-bayanihan-act-most-dangerous/

A few days after the law was signed, there were 32 arrests related to "fake news"[90] proving that the fear of the fake news provision being used to suppress free speech was not unfounded. Interestingly, many of these arrests did not make use of the Bayanihan law but were still based on violations of the Revised Penal Code (i.e., "Unlawful Use of Means of Publication and Unlawful Utterances"). The provision on false information was omitted in the subsequent versions of the Bayanihan law.

Most of these arrests were those of ordinary citizens airing their complaints on social media. These citizens were arrested either for charges of cyberlibel or under the justification of spreading "fake news." For instance, a public school teacher from General Santos City was arrested without a warrant after venting that people from her city were going hungry and encouraging people with nothing to eat to raid the local gym, where undistributed food packs meant for them were stocked. Her son was also arrested for trying to stop the police from taking his mother without a warrant. The teacher was charged with inciting to sedition in relation to the cybercrime law, as she posted her rant on social media.[91] Human rights groups immediately opposed this arrest, calling it an overkill as the teacher was simply airing her legitimate grievances over her local government's unsatisfactory COVID response that led to mass hunger.[92] In another instance, a private individual was subpoenaed for a post made about the misuse of local government funds for COVID relief.[93] A salesman was arrested in Agusan del Norte for calling then-President Duterte "stupid" and "crazy" in his local language in his Facebook comments. In the same week, at least four arrests were made against social media users who posted comments critical of Duterte.[94] The then-Secretary of Interior and Local Government filed charges against an administrator of a Facebook page for attributing a false quote to him regarding physical distancing measures.[95]

Even campus journalists were not spared from intimidation. An editor of a college publication was red-tagged and threatened by the police after publishing critical opinions on the Duterte administration's COVID-19 response. The campus journalist's Facebook account was also probed by the police.[96] Another campus publication in Cebu was publicly called out – via Facebook – by the Cebu governor after it criticized her creation of a special unit specifically tasked to trace individuals who post negative criticisms about the government's COVID-19 response.[97]

90 32 arrested over 'fake' COVID-19 news," *CNN Philippines*, April 6, 2020, https://www.cnnphilippines.com/news/2020/4/6/arrests-over-coronavirus-fake-news.html

91 "Teacher, son arrested without warrant in GenSan over Facebook post," *Rappler*, March 28, 2020, https://www.rappler.com/nation/256157-teacher-son-arrested-without-warrant-general-santos-city-facebook-post-coronavirus/

92 "Human rights group calls for release of teacher arrested over 'seditious' Facebook post," *CNN Philippines*, March 29, 2020, https://www.cnnphilippines.com/news/2020/3/29/karapatan-teacher-arrest-sedition-charges-coronavirus.html

93 "Chilling effect: NBI going after netizens for social media posts on COVID response - Diokno" *ABS-CBN News*, April 2, 2020, https://news.abs-cbn.com/news/04/02/20/chilling-effect-nbi-going-after-netizens-for-social-media-posts-on-covid-response-diokno

94 "Salesman arrested for social media post against Bong Go, Duterte," *CNN Philippines*, May 14, 2020, https://www.cnnphilippines.com/news/2020/5/14/Duterte-cyberlibel-arrest-Agusan-del-Norte.html

95 "Palace defends socmed monitoring," *Manila Standard*, September 8, 2020, https://www.manilastandard.net/news/top-stories/333555/palace-defends-socmed-monitoring.html

96 Consuelo Marquez, "CEGP condemns alleged 'red-tagging' of campus journalist," *Inquirer.net*, April 5, 2020, https://newsinfo.inquirer.net/1254285/cegp-condemns-alleged-red-tagging-of-campus-journalist

97 Delta Dyrecka Letigio, "CEGP cries foul over Gwen's reply to school pub's statement," *Cebu Daily News*, March 25, 2020, https://cebudailynews.inquirer.net/296967/cegp-cries-foul-over-gwens-reply-to-school-pubs-statement

VII. Analysis

A. The Right to Privacy and Right to Information are Essential to a Comprehensive Definition of Civic Space

CIVICUS defines civic space as "the place, physical, virtual, and legal, where people exercise their rights to freedom of association, expression, and peaceful assembly."[98]

In this initiative, we propose a more comprehensive definition of civic space that includes not just the freedom of association, expression, and assembly, but also the right to privacy and access to information. Apart from being fundamental rights recognized by the International Covenant on Civil and Political Rights, the rights to privacy and information are essential for people to participate in civic space fully and meaningfully. The right to privacy gives people the autonomy and agency over their bodies, their possessions, and their data, and therefore gives them the freedom to speak out on issues of public concern and participate in public decision making.

Discussions on shrinking civic spaces must also address the fact that many cases of state violence against journalists and activists are preceded by privacy violations such as stalking, monitoring, and unauthorized use of personal information. Thus, attacks on privacy and anonymity must be interrogated for more than just their virtual harms but must be seen as attempts to stifle civic freedoms in physical spaces.

Source: Jurgen Jester, Pexels
Surveillance Cameras on a Metal Post.

...the rights to privacy and information are essential for people to participate in civic space fully and meaningfully. The right to privacy gives people the autonomy and agency over their bodies, their possessions, and their data, and therefore gives them the freedom to speak out on issues of public concern and participate in public decision making.

98 "Guide to Reporting on Civic Space: Media Toolkit," CIVICUS, https://www.civicus.org/index.php/media-resources/resources/toolkits/2746-guide-to-reporting-civic-space

B. Modern Surveillance is Exercised through the Erosion of Anonymity

Traditionally, the notion of surveillance pertains to the activity of active monitoring. However, another aspect of surveillance is the chilling effect that is caused by its mere presence. In explaining Panopticism, Foucault discusses how the constant monitoring and examination of activities becomes a means by which power is exercised and self-censorship is encouraged. In a Panopticon, it doesn't matter whether the actual exercise of surveillance is a continuous one; it only matters that the surveillance apparatus is in place. Hence, "a state of conscious and permanent visibility that assures the automatic functioning of power."[99] In the modern age, this is manifested in the mere establishment of surveillance measures and legislation, notwithstanding the implementation or the effectiveness of such measures, as their mere existence pushes people to self-regulate for fear of being apprehended. This includes measures that place citizens' identities on such close view by the State, such as real-name policies, SIM card and social media registration, and the continuous collection of personal data and creation of databases through ID systems like the PhilSys.

In online spaces, the most common manifestation of this panopticon-esque model of surveillance is the erosion of anonymity, which forces people to self-regulate as their identities are always on display. Certain sectors of civil society such as queer activists are in higher danger of being disenfranchised by these surveillance measures due to their reliance on anonymous platforms to express their lived identities, as opposed to the legal identities that real-name policies force on internet users.

C. The Propensity of Social Media Algorithms towards Creating and Maintaining Echo Chambers and Filter Bubbles are Shrinking Spaces for Deliberative Discourse Online

Disinformation research has shown that the niche communities and filter bubbles encouraged by the way social media platforms like Facebook are designed, contribute to the rapid spread of disinformation and even hate speech in the same platforms. The closed and private nature of these groups also often make it close to impossible for those outside them to report violations, and for the platforms to monitor and regulate activity within the groups. This raises the need to question whether companies like Meta are genuinely expanding spaces for discourse and increasing people's means of political participation through products such as Free Facebook. We make the case that contrary to their claims, platforms like Facebook are, in fact, shrinking the spaces for deliberation and discourse because of how their algorithms are designed to encourage polarization and maintain the existence of filter bubbles and echo chambers. This is especially critical in the case of the Philippines due to the increasing reliance of Filipinos on social media, particularly on Facebook, for news and knowledge that inform their political participation.

99 Michel Foucault, ""Panopticism" from *Discipline & Punish: The Birth of the Prison," Race/Ethnicity: Multidisciplinary Global Contexts 2*, no. 1 (Autumn 2008): 1-12, https://muse.jhu.edu/article/252435

D. Digital Technologies Blur the Line between Public and Private, thus bringing to Question Traditional Notions of Safety and Security

One of the oldest debates about online platforms, especially social media networks, is whether social media platforms are public or private spaces. Existing Philippine jurisprudence leans towards the former. In the landmark case of *Vivares vs. St. Theresa's College*, the Philippine Supreme Court ruled that a reasonable expectation of privacy cannot be automatically assumed in online social networking platforms such as Facebook. The decision states that for one to have an expectation of privacy when using social networking platforms, "it is first necessary that said user [...] manifest the intention to keep certain posts private, through the employment of measures to prevent access thereto or to limit its visibility."[100] Simply put, prevailing local jurisprudence says that social media platforms are public platforms by default, and it is only by utilizing the platform's privacy settings that users can assert a reasonable expectation of privacy over their activity and the content that they upload in the platform. However, vulnerable groups such as victims of domestic violence and the LGBTQ community often take to online spaces to find refuge and safety.

This blurring of lines became even more evident during the COVID-19 pandemic, when restrictions to mobility forced everyone to shift into online modes of public participation. This also meant that physical spaces and communities that used to be safe spaces for women to speak out against abuse were dissolved and shifted to digital channels of communication.

E. In the Philippines, Threats to Civic Space are Reinforced by Poor Quality of Internet and Weak Internet Governance

Disinformation and the lack of access to diverse and factual information are exacerbated by the fact that internet quality remains dismal in many parts of the country.

Lack of quality internet access pushes people in far-flung areas and low-income communities to rely on affordable platforms such as free television for news and for the exercise of their civil and political rights. However, the attacks on traditional media have decreased both trust and access to a major provider such as ABS-CBN, thus leaving some demographic groups with little to no sources of credible and accurate information. The longstanding market capture of two major telecommunications and internet service providers in the country has hampered improvement on the quality, speed, and affordability of Philippine internet, thus leaving some users with no other choice than to rely on affordable "mobile internet bundles" that limit their access to one or a few social media sites such as Facebook and YouTube.

100 G.R. No. 202666, *Vivares vs. St. Theresa's College*, September 29, 2014, https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/1/57754

The systems-first approach to cybersecurity (i.e., one that prioritizes the security of systems over the security of persons) is a threat to civic space as it can be used by governments to justify measures that violate civic freedoms under the guise of securing critical information infrastructures.

This is complemented by the fact that discussions on ICT-related policies in the Philippines remain mostly exclusive to government and private sector voices, leaving marginalized sectors and communities unheard and disempowered by treating them as passive consumers.

The problem with cybersecurity, as with other forms of security, is that it is often regarded as a panacea to every problem in cyberspace. But not all cyber threats are cybersecurity threats. Information disorders are not necessarily security threats (although they can eventually be so). What is therefore crucial for both policymakers and civil society is to build a more nuanced understanding of digital issues and their links to offline ones. Moreover, to counter securitization as a knee-jerk response to disinformation, information disorders must be viewed not as mere cybercrimes, but as a systemic disease that goes beyond the online realm and plagues many, if not all, facets of democracy. This should involve a holistic approach and more inclusive policy making processes, even in areas that are usually deemed too technical for open public consultations.

The systems-first approach to cybersecurity (i.e., one that prioritizes the security of systems over the security of persons) is a threat to civic space as it can be used by governments to justify measures that violate civic freedoms under the guise of securing critical information infrastructures.

To counter securitization as a knee-jerk response to disinformation, information disorders must be viewed not as mere cybercrimes, but as a systemic disease that goes beyond the online realm and plagues many, if not all, facets of democracy.

VIII. Strategies of Resistance and Levers of Change

Online platforms have been powerful tools for resistance against repressive laws and policies. When the Anti-Terrorism Bill of 2020 was approved on final reading despite numerous concerns about both its content and the way it was railroaded in the House of Representatives, Filipinos took to the streets and to social media to call on lawmakers to scrap the bill using the hashtags #junkterrorbill and #junkterrorbillnow. Online signature campaigns were launched, and online users were urged to send emails to their respective representatives for the same purpose. The calls soon garnered international attention, with then-United Nations High Commissioner for Human Rights Michelle Bachelet issuing a warning against the dangers of the legislation, and international pop star Taylor Swift sharing a link to the online petition against the proposed law.[101] The public clamor against the bill was so loud that some lawmakers eventually withdrew their authorship of the bill, while some who were originally named as co-authors denied their involvement.[102]

Philippine civil society has utilized various strategies to push back against the digital threats to civic space, as identified earlier in this paper. Most importantly, alternative visions and definitions of safety and security are cropping up in several pockets of civil society, both globally and in the Philippines. This last section looks at these alternative strategies and counter-narratives that could be considered as new pathways for the preservation of a free civic space.

A. Global Movement for People-centric Cyber Policy

In the international arena, civil society has been pushing back against the creation of oppressive and exploitative global norms by building alliances and making concerted efforts to increase civil society participation in spaces that are traditionally exclusive to State and corporate actors. One such space is the UN Open Ended Working Group on security of and the use of information and communications technologies. Through active participation by digital rights groups and networks such as the Association for Progressive Communications, the global human rights movement has repeatedly raised the need for the inclusion of human rights and marginalized voices in cyber norms.[103] There is also a growing global movement for digital constitutionalism, which is comprised of "constitutional counteractions against the challenges produced by digital technology," described as "the ideology that adapts the values of contemporary constitutionalism to the digital society."[104]

101 Barnaby Lo, "Protest against 'urgent' anti-terror bill in Philippines gets a boost from Taylor Swift," *CBS News*, June 4, 2020, https://www.cbsnews.com/news/protest-against-urgent-anti-terror-bill-in-philippines-gets-a-boost-from-taylor-swift/

102 Catalina Ricci S. Madarang, "These lawmakers withdrew support for Anti-Terror Bill after initially backing it," *Interaksyon*, June 4, 2020, https://interaksyon.philstar.com/politics-issues/2020/06/04/169972/these-lawmakers-withdrew-support-for-anti-terror-bill-after-initially-backing-it/

103 Verónica Ferrari and Sheetal Kumar, "A human centric approach to international cybernorms: Civil society feedback on the UN Open-Ended Working Group on ICTs proposals," Association for Progressive Communications, December 1, 2020, https://www.apc.org/en/news/human-centric-approach-international-cybernorms-civil-society-feedback-un-open-ended-working

104 Edoardo Celeste, "Digital constitutionalism," *International Review of Law, Computers & Technology 33*, no. 1 (2019): 76-99, https://doi.org/10.1080/13600869.2019.1562604

B. Local Initiatives for Inclusive and Civil Society-led Internet Governance

The global call for a multistakeholder approach to internet governance is reflected in local initiatives like the Philippine Declaration on Internet Rights and Principles and the Magna Carta for Philippine Internet Freedom, which both stem from the dissatisfaction of Philippine civil society with the Cybercrime Prevention Act of 2012.

Recognizing the growing threats to digital rights and the lack of civil society voices in internet governance, various stakeholders created the Philippine Declaration on Internet Rights and Principles in 2015. It presents an alternative vision of the internet – one that puts the rights and needs of the Filipino people at the center.[105] The Declaration was a product of collective drafting and consultations with civil society internet rights groups and the ICT policy community and was largely inspired by similar initiatives such as the Marco Civil da Internet in Brazil (Brazilian Civil Rights Framework for the Internet). Apart from its progressive approach to internet governance in that it lays down as bases the rights of users instead of focusing on the interests of internet companies or law enforcement, the Marco Civil is known to have gone through a thorough public consultation process, including online forms of consultation.[106]

Similarly, the Magna Carta for Philippine Internet Freedom (MCPIF), which was first filed as a Senate Bill during the 15th Congress in 2012, was designed as a rights-based replacement to the Cybercrime Prevention Act. Like the Marco Civil da Internet, the MCPIF bill was "crowdsourced" in that the drafting process was made accessible to the public through official online platforms.[107] Unlike the existing cybercrime law, the MCPIF treats libel as a civil liability rather than a criminal act and guarantees the right against illegal searches and seizures by providing strict guidelines for any collection of data.[108]

C. Rights-based Strategic litigation

When the cybercrime law was first passed in 2012, it caused a massive uproar among the Filipino public because of its controversial provisions that restrict free speech and infringe on the constitutional right to privacy. A partial victory was achieved by the movement when in the case of Disini v. The Secretary of Justice, the Supreme Court declared as unconstitutional some of the provisions that were questioned by human rights advocates, namely:

a. *Section 4(c)(3) of Republic Act 10175 that penalizes the posting of unsolicited commercial communications;*

b. *Section 12 that authorizes the collection or recording of traffic data in real-time; and*

c. *Section 19 that authorizes the Department of Justice to restrict or block access to suspected Computer Data.*

105 "The Philippine Declaration on Internet Rights and Principles," Foundation for Media Alternatives, https://fma.ph/ph-declaration-internet-rights-principles/

106 Mariana Valiente, Dennys Antonialli, and Francisco Brito Cruz, "Marco Civil 5 Years Special: Why should we celebrate?," *Internet Lab*, April 3, 2019, https://internetlab.org.br/en/news/marco-civil-5-years-special-why-should-we-celebrate/

107 Jonathan De Santos, "The Wisdom of Crowds: Crowdsourcing Net Freedom," *Vera Files*, January 21, 2013, https://ph.news.yahoo.com/blogs/the-inbox/wisdom-crowds-crowdsourcing-net-freedom-042242158.html

108 "Magna Carta for Internet Freedom to Replace Anti-Cybercrime Law — Miriam," Senate of the Philippines, November 30, 2012, https://legacy.senate.gov.ph/press_release/2012/1130_santiago1.asp

Although contentious provisions such as the criminalization of cybersex and cyberlibel were upheld, the decision is key to ensuring that the surveillance powers of law enforcement are kept within the bounds of the Philippine Constitution.

The recent case filed by independent media organizations over the DDoS attacks on their websites was a powerful statement against the excessiveness of the cybercrime law. Instead of filing a criminal case based on the Cybercrime Prevention Act, the parties opted to file a civil complaint against the IT companies named in the digital forensics report. The complaint was based on Article 32(3) of the Civil Code, which protects the freedom of Filipinos to write for the press or to maintain a periodical publication.[109] In the succeeding year, *Altermidya* network members filed another complaint, this time against the National Task Force to End Local Communist Armed Conflict (NTF-ELCAC) for multiple instances of red-tagging.[110] These legal actions are valuable because they demonstrate that cyberlibel is extremely redundant and unnecessary, especially at a time when libel (online or otherwise) has become a political weapon more than anything else.

This case is also an exemplary demonstration of the value of global solidarity among civil society in countering oppressive governments. The alternative media organizations were able to mitigate the cyber-attacks and produce a digital forensics report that became the basis of their civil complaint through the assistance of Qurium Media Foundation, the non-profit organization based in Sweden.

When the National Telecommunications Commission ordered the blocking of several websites that, according to them, were linked to terrorist groups, the order was immediately assailed in court by the independent media groups unduly included in the block list. Independent media outlets *Bulatlat* and *Pinoy Weekly* were not notified in advance that their websites would be blocked. *Bulatlat's* petition for the issuance of a temporary restraining order against the NTC memorandum was originally denied by the Regional Trial Court on the basis that *Bulatlat* could still publish online and that the inconvenience caused by the blocking is "of no moment" and "irrelevant."[111] However, *Bulatlat's* petition for a preliminary injunction against the blocking order was eventually granted by the court upon finding that a 44% drop in monthly site traffic meant that readers, writers, and contributors were denied access to information which amounted to a restriction of the constitutionally protected right to freedom of speech.[112] When, despite the issuance of a writ of preliminary injunction that ordered the unblocking of *Bulatlat's* sites, NTC still continued to block the website, *Bulatlat* asked the court to hold the NTC in contempt. Throughout this lengthy process, *Bulatlat* was represented by lawyers from the National Union of People's Lawyers, a voluntary association of human rights lawyers in the Philippines.[113]

109 "Alternative media groups file civil case amid cyberattacks," *Rappler*, March 29, 2019, https://www.rappler.com/technology/226968-alternative-media-groups-file-civil-case-cyberattacks-march-2019/

110 Kristine Joy Patag, "Alternative media groups sue NTF-ELCAC over continued red-tagging," *Philstar.com*, December 18, 2020.

111 "After denying TRO, what's next in the fight to #UnblockBulatlat?," *Bulatlat*, July 14, 2022, https://www.bulatlat.com/2022/07/14/after-denying-tro-whats-next-in-the-fight-to-unblockbulatlat/

112 "Philippines: Court orders NTC to unblock Bulatlat website," *International Federation of Journalists*, August 16, 2022, https://www.ifj.org/media-centre/news/detail/category/press-releases/article/philippines-court-orders-ntc-to-unblock-bulatlat-website.html

113 Jairo Bolledo, "Bulatlat asks QC court: Hold NTC in contempt for delaying unblocking of site," *Rappler*, August 25, 2022, https://www.rappler.com/nation/bulatlat-asks-court-hold-ntc-contempt-not-immediately-unblocking-website/

D. Civil Society-led Cyber Incident Response

The experience of Philippine alternative media groups in responding to cyberattacks on their websites is demonstrative of the lack of local capacity for cyber incident response. In most, if not all of the cyberattacks described in this paper, local groups have had to rely on foreign entities such as the Qurium Media Foundation to conduct digital forensics and emergency response to secure their websites and systems. While global non-profits such as Qurium and Access Now provide digital security resources for activists, it is critical to build the internal capacity of local organizations and strengthen their first line of defense against attacks on their digital assets.

E. Feminist and Queer Approaches to Safety and Security

As frequent targets of harassment, abuse, misogynistic remarks and other forms of gender-based violence, women and queer persons are often disenfranchised by lacking or disproportionate responses to online threats. But feminist movements are replete with alternative visions of a safe and free internet. In the Philippines, the Safe Spaces Act, passed in 2018, aims to prevent and penalize gender-based harassment in both physical and online spaces.

As frequent targets of harassment, abuse, misogynistic remarks and other forms of gender-based violence, women and queer persons are often disenfranchised by lacking or disproportionate responses to online threats. But feminist movements are replete with alternative visions of a safe and free internet.

Source: Photo by Raffy Lerma
Employees, journalists, celebrities, and supporters of media network ABS-CBN show their dissent a week after Congress rejected their franchise renewal with a noise barrage and motorcade outside the ABS-CBN compound in Quezon City on July 18, 2020.

It defines gender-based online sexual harassment as:

> *acts that use information and communications technology in terrorizing and intimidating victims through physical, psychological, and emotional threats, unwanted sexual, misogynistic, transphobic, homophobic, and sexist remarks and comments online whether publicly or through direct and private messages, invasion of victim's privacy through cyberstalking and incessant messaging, uploading and sharing without the consent of the victim, any form of media that contains photos, voice, or video with sexual content, any unauthorized recording and sharing of any of the victim's photos, videos, or any information online, impersonating identities of victims online or posting lies about victims to harm their reputation, or filing false abuse reports to online platforms to silence victims.*[114]

By specifically naming misogynistic, transphobic, homophobic, and sexist remarks as forms of online harassment, the law becomes inclusive not just of the experiences of women, but also those who identify as part of LGBTQ.

Filipino feminist and queer organizations also operationalize their own narratives and visions of safety through initiatives such as the Lunas Collective, a Facebook-based chat service providing support for those who experience gender-based violence.[115] By carving out safe spaces for themselves and for women, these organizations are able to turn the community features of platforms such as Facebook into spaces of solidarity and support rather than breeding grounds of disinformation and misogyny.

114 Republic Act No. 11313, Safe Spaces Act, https://pcw.gov.ph/republic-act-11313/

115 Cody Cepeda, "Lunas Collective: Keeping the distance that COVID-19 social distancing removes between abuser, abused," Inquirer.net, April 3, 2020, https://newsinfo.inquirer.net/1253503/lunas-collective-keeping-the-distance-that-covid-19-social-distancing-removes-between-abuser-abused

Women journalists who, as the case of Maria Ressa demonstrates, are particularly vulnerable to online violence – are also coming together to create their own virtual safe spaces. A few days after the Supreme Court upheld the constitutionality of the Anti-Terrorism Law, the International Association of Women in Radio and Television launched Digital Safe House, an online platform where women journalists can report cases of attacks, harassment, abuses, and other gender-based violence, and access resources and services such as legal and medical assistance.[116]

Women and girls in the Philippines have been reclaiming online spaces as safe spaces for telling their stories and demanding accountability from abusers and sexual predators, mostly through hashtag campaigns.

At the height of the pandemic in 2020, the hashtag #HijaAko ("I am *hija*") became a trending topic after a young female celebrity spoke out against TV host Ben Tulfo for saying that the way women dress invites sexual offenders to commit crime.[117] Shortly after this, students and alumni of Miriam College took to social media to share their personal accounts of sexual harassment by faculty members of the said school, using the hashtag #MCHSdobetter.[118] This triggered a chain of similar hashtags by students and alumni from other schools exposing patterns of sexual misconduct by teachers and holding perpetrators of sexual assault to account.

Women and girls in the Philippines have been reclaiming online spaces as safe spaces for telling their stories and demanding accountability from abusers and sexual predators, mostly through hashtag campaigns.

Other strategies that could be explored to resist the Philippine government's digital security playbook are breaking the monopoly of Facebook by migrating into other secure online platforms; investigating surveillance trade and the use of surveillance technologies by the Philippine government; and pushing for oversight and accountability both by state actors and global tech companies that wield so much unregulated power over cyberspace.

Finally, there is a need to debunk the image of the Philippines as being a suitable "petri dish" for the abuse of technology by businesses and governments. While the Duterte administration attempted to build an arsenal of repressive laws, practices, and technologies, democracy also has its own toolbox in the form of regulations and mechanisms, as well as emergent innovative strategies by civil society that are designed to protect citizens in their use of digital technologies. The challenge is now in wielding these tools to uphold a free civic space.

116 Group launches 'Digital Safe House' for Filipino women journalists," *Bulatlat*, December 13, 2021, https://www.bulatlat.com/2021/12/13/digital-safe-house-for-filipino-women-journalists-launched/

117 Pilar Manuel, "#HijaAko trends after Frankie Pangilinan hits back at Ben Tulfo for victim-blaming women," *CNN Philippines*, June 14, 2020, https://www.cnnphilippines.com/entertainment/2020/6/14/Frankie-Pangilinan-Ben-Tulfo-victim-blaming-women.html

118 "#MCHSdobetter: Groups condemn sexual misconduct of teachers, call for justice," *Rappler*, June 26, 2020, https://www.rappler.com/moveph/264962-groups-condemn-sexual-misconduct-teachers-call-justice/

About Civic Futures

Civic Futures is a philanthropic initiative conceptualised and launched by the Funders Initiative for Civil Society (FICS) which acts as its secretariat and the Fund for Global Human Rights (FGHR) which is a founding member. Civic Futures exists to mobilize the funding community working across multiple issue areas to equip civil society to push back against the overreach of national security and counter-terrorism powers, increasingly used by governments around the world to harm civic space.

DOI: 10.5281/zenodo.7789243

civicfutures@global-dialogue.org
civic-futures.org

Civic Futures