stratbase
+
ADRi PUBLICATIONS

THE WEST PHILIPPINE SEA
AND THE CONVERGENCE OF OFFENSIVE CYBER AND DISINFORMATION ACTIVITIES

SHERWIN E. ONA, PH.D.

The Stratbase ADR Institute for Strategic and International Studies (ADRi) is an independent strategic research organization with the principal goal of addressing the issues affecting the Philippines and East Asia through:

1. Effecting national, regional, and international policy change or support
2. Fostering strategic ideas based on cooperation and innovative thinking
3. Providing a regional venue for collaboration and cooperation in dealing with critical issues in East Asia; and
4. Actively participating in regional debates and global conversations

With its international focus, ADRi believes that Philippine and regional security and development can be achieved through the cooperation of the public and private sectors.

ADRi traces its roots to the Stratbase Research Institute (SRI) established in 2004. SRI focused on providing strategic solutions to domestic governance, socio-economic, and other policy concerns. It aimed to contribute to Philippine development through research and responsive policy alternatives.

As SRI sought solutions, East Asia's affairs frequently inserted themselves into the equation. There was and is a clear relation between domestic and regional affairs; movement in one reverberates in the other.

THE WEST PHILIPPINE SEA AND THE CONVERGENCE OF OFFENSIVE CYBER AND DISINFORMATION ACTIVITIES

WRITTEN BY
SHERWIN E. ONA, PH.D.

stratbase +ADRi PUBLICATIONS
STRATBASE ADRi FOR STRATEGIC AND INTERNATIONAL STUDIES
Manila, Philippines

Stratbase ADRi
Albert Del Rosario Institute for Strategic and International Studies

A Publication of the Stratbase Albert Del Rosario Institute for
Strategic and International Studies

Stratbase ADRi Website: www.adrinstitute.org
Facebook: https://facebook.com/stratbaseadri/
Twitter: https://twitter.com/stratbaseadri/

The views, opinions and conclusions expressed in this paper are those of the author and do not necessarily reflect those of the Institute or any of its officers and trustees.

The author is solely responsible for its content.

For information, address ADRi Publications:
The Financial Tower, 6794 Ayala Avenue, Makati City 1226

Design by Carol Manhit
Text set in 11 type Minion Pro

ABOUT THE ORGANIZATION

Victor Andres "Dindo" C. Manhit is the President of Stratbase Albert Del Rosario Institute for Strategic and International Studies. Concurrently, he is Philippine Country Head of the renowned BowerGroupAsia (BGA). He was a former Chair and recently retired Associate Professor of the Political Science Department of De La Salle University. Among the government positions he held include Undersecretary for External Affairs and Special Concerns of the Department of Education, Culture and Sports and Deputy Secretary for Administration and Financial Services of the Philippine Senate. Meanwhile, his legislative experience encompasses the 8th, 9th, 10th, and 12th Congress as the Chief of Staff of the late Former Senate President Edgardo Angara and senior policy research adviser in key senate committees.

BOARD OF TRUSTEES

Ambassador Albert del Rosario was the Secretary of Foreign Affairs of the Philippines from 2011 to 2016. He also served as Philippine Ambassador to the United States of America from 2001 to 2006. Prior to entering public service, Amb. Del Rosario was on the Board of Directors of over 50 firms. He received numerous awards and recognition for his valuable contributions to the Philippines and abroad.

Manuel V. Pangilinan is CEO and managing director of First Pacific Company Limited. He is also the chairman of Metro Pacific Investments Corp., Philippine Long Distance Telephone Company, Manila Electric Co. (Meralco), and Smart Communications, among others. He is a recipient of several prestigious awards including the Ten Outstanding Young Men of the Philippines (TOYM) Award for International Finance in 1983 and the Presidential Pamana ng Pilipino Award by the Office of the President of the Philippines in 1996.

Edgardo G. Lacson is an honorary chairman of the Philippine Chamber of Commerce and Industry (PCCI). He is the Chairman of the Employers Confederation of the Philippines. He holds numerous leadership positions in various companies. He served as a Director of The Philippine Stock Exchange, Inc. and is an Honorary Member of the Rotary Club-Diliman.

Benjamin Philip G. Romualdez is the former president of the Chamber of Mines of the Philippines. He also holds, among others, the following positions: Chairman of MST Management, Inc., President of Oxford University and Cambridge University Club of the Philippines, Director at Philippine-Australia Business Council (PABC), Trustee/Vice President of Doña Remedios Trinidad Romualdez Medical Foundation, Inc, and Trustee/Vice President of Dr. Vicente Orestes Romualdez (DVOR) Educational Foundation, Inc.

Ernest Z. Bower is a senior adviser for Southeast Asia at the Center for Strategic and International Studies (CSIS), having founded the first chair for the region. He is CEO of BowerGroupAsia (BGA) and a leading expert on Southeast Asia.

Renato C. de Castro, Ph.D is a full professor of international studies at De La Salle University – Manila (DLSU). In 2009, Dr. de Castro became the U.S. State Department ASEAN Research Fellow from the Philippines and was based in the Political Science Department of Arizona State University. A consultant in the National Security Council of the Philippines during the Aquino administration, he has written over 80 articles on international relations and security.

Judge Raul C. Pangalangan, Ph.D is a judge of the International Criminal Court. He was previously the dean of the University of the Philippines College of Law and publisher of the Philippine Daily Inquirer. He has taught in many universities around the world, such as Melbourne University, Hong Kong University, and Harvard Law School.

Epictetus E. Patalinghug, Ph.D is a professor emeritus at the Cesar E.A. Virata School of Business, University of the Philippines (UP), Diliman. He received his doctorate degree in Agricultural Economics from the University of Hawaii. His works have been featured in various publications around the world.

Francisco A. Magno, Ph.D is the executive director of the Jesse M. Robredo Institute of Governance and former President of the Philippine Political Science Association. He is a professor of political science at DLSU and previously served as Chair of the Political Science Department and Director of the Social Development Research Center.

Carlos Primo C. David, Ph.D is a licensed geologist and professor in UP Diliman having obtained his PhD in Environmental Science and Geology from Stanford University. He is a former the Executive Director of DOST-PCIEERD. A project leader of the DOST's Project NOAH, Dr. David pioneers short term rainfall forecasting in the country and climate change-related research on water resources. (On government service leave)

CONTENTS

ABSTRACT

The country's current strategy in the West Philippine Sea (WPS) involves enhancing its diplomatic, economic, and security collaboration with its allies. There is also a renewed sense of urgency to develop its defense capabilities and foster cooperation with several ASEAN member states. However, these efforts drew a sharp rebuke from China. Combined with its stern warnings and provocative actions in the WPS, its alternative narratives are vigorously propagated in cyberspace through traditional and social media. For instance, Facebook and YouTube accounts of alleged Chinese sponsored propagandists accuse the Philippine Coast Guard of unprofessional conduct at sea leading to several collisions in Ayungin shoal. Furthermore, its disinformation activities are often combined with cyber-attacks on government and economic targets. Beijing's belligerent actions in cyberspace illustrate a convergence of offensive cyber operations and disinformation activities that is intended to advance a broader malign influence agenda. This also reveals its alleged strategic goal of establishing information dominance by controlling the narrative and weakening an adversary's resolve by sowing confusion, undermining its institutions, and fostering societal division. Given these challenges, it is crucial for the Philippines to understand how foreign malign influence through digitally enabled convergence strategies are operationalized. For this reason, the study examined this phenomenon by plotting incidents and established a timeline combined with the messaging themes related to the WPS issue. To further understand the context of such campaigns, the study will also discuss the offensive cyber and disinformation operations in Hong Kong and Taiwan. Finally, the paper provides Filipino decision makers and security planners with options on how to mitigate the adverse effects of these malign activities. These recommendations underscore the need for a whole of society approach that entails the development of policies on cyber defense and digital literacy. It is also crucial to harness the best practices from the private sector, academic institutions, and civil society organizations as well as leverage the country's international partnerships. More importantly, with the appropriate policies and programs, the Philippines must ensure the resilience of its people and institutions to overcome these challenges.

THE WEST PHILIPPINE SEA AND THE CONVERGENCE OF OFFENSIVE CYBER AND DISINFORMATION ACTIVITIES

SHERWIN E. ONA, PH.D.

Early in its conception, cyber operations and information warfare were two distinct fields. Clear lines were established not only in its doctrines but also in training, and its employment. However, the rapid developments in digital technologies coupled with the weaponization of cyberspace have blurred these boundaries. Today's geopolitical situation shows a convergence of these fields, resulting in the creation of strategies that combine offensive cyber capabilities and cyber-enabled disinformation activities. The strategic intent behind this convergence is to spread malign influence using it as the preferred weapon. In this scenario, malicious actors work to achieve their desired outcomes by fomenting distrust, sowing division, and undermining their adversary's decision-making capacities. Unfortunately, this insidious concoction of doctrine, strategy, and actions reveals its form in the Philippines. This is shown in China's increasing assertiveness in the West Philippine Sea (WPS) where its maritime actions are combined with the vigorous spread of false narratives in both online and traditional media. For instance, Facebook accounts linked to alleged People's Republic of China (PRC) propagandists and troll farms continue to push false claims about the untoward incidents involving the Philippine Coast Guard (PCG) and Chinese Coast Guard (CCG) as well as its maritime militia. Moreover, the rise in cyberattacks against public agencies appears to be linked to these insidious activities. Fortunately, this precarious situation has provided valuable insights into the operationalization of offensive cyber and disinformation activities. A 2021 study by the RAND Corporation alleged that China spends USD10 billion annually on cyber and information operations. In addition, the People's Liberation Army (PLA) has an elaborate cyber-information warfare structure under its Strategic Support Force. It is organized to cover 5 theatres of operations with 12 bureaus, 14 offices, and numerous working groups. Several of these units are labeled as civilian organizations (Harold et al, 2021). Moreover, a 2021 estimate places the size of China's cyber army at around 170,000 (Newsweek, 2024). It is also alleged that millions of Chinese civilians are recruited for this effort through monetary incentives. For instance, the purported existence of a 50-cent keyboard army refers to cyber recruits who are given .50 yuan (7.02USD) per post (Twigg & Allen, 2021). In addition, the Chinese Communist Party's influence operations are being overseen by the United Front Work Department (UFWD) which is responsible for controlling its network of proxies and front organizations to advance Beijing's strategic intent (Chalk, 2023). It uses intimidation, surveillance, and coopting techniques to target ethnic Chinese communities, business organizations, politicians, as well as student groups with the goal of winning the hearts and minds of its target audience and mitigating criticism (Searight, 2020). Other state agencies like the Ministry of State Security and the Ministry of Public Security are also part of this massive campaign.

For its disinformation efforts in the South China Sea (SCS), much emphasis is placed on presenting a counter-narrative that undermines the Philippine claim. It also intends to change the public perception by fostering uncertainty and confusion. Furthermore, the Taiwan Straits issue also figures prominently in this campaign. The activities related to this are more focused on dissuading its government from declaring the island's independence. Thus, it is common to see disinformation that undermines the credibility of the Taiwanese government as well as the use of intimidation to instill fear of an invasion. In addition, Hong Kong is another case that can provide valuable insights into how social media figured prominently in disinformation activities against the pro-democracy protest. In these cases, it is noticeable that the increase in disinformation activities coincides with a surge in cyberattacks against government agencies and public personalities.

Given the dangerous and widespread nature of these activities, the study examines the convergence of offensive cyber and disinformation activities as part of foreign malign influence operations. It is also crucial for the Philippines to adopt a coherent strategy that will address this imminent threat and guard against these malign activities. Moreover, addressing these challenges requires an understanding of an adversary's intent and context. For this purpose, the study aims to provide decision makers and security planners with options on how to mitigate its effects through the following objectives:

a. *Establish the common themes and sources related to disinformation and cyberattacks surrounding the WPS issue*

To do this, news reports detailing the aggressive actions of the CCG and its militia arm covering the January to December 2023 period were collated. Afterwards, reports that were inconsistent with these accounts were identified as disinformation examples. These items were further classified into themes. Cyberattacks based on news reports were also used to illustrate their connection with disinformation activities.

b. *Draw lessons from similar events in Taiwan and Hong Kong*

For this objective, the study relied on secondary sources such as technical reports, research papers and news items to provide a compelling picture of the threat environment.

c. *Propose policy related actions that address foreign malign influence activities*

Based on the lessons learned from objectives (a) and (b), the paper enumerates several recommendations on how the Philippines can mitigate these challenges.

The paper does not intend to provide an exhaustive list of offensive cyber and disinformation activities related to the WPS. Rather, the study presents examples of the convergence of these actions and argues that this trend can ultimately lead to a broader malign influence agenda. Also, further research is recommended to enable policy makers to "connect the dots" and craft appropriate actions.

Background Discussion

The country's current strategy in the WPS involves enhancing its diplomatic, economic, and security collaboration with the United States and other like-minded democracies. It has also embarked on a recalibrated modernization program for the Armed Forces of the Philippines (AFP) and the PCG. Furthermore, there is also a renewed sense of urgency to foster cooperation with several ASEAN member states. This policy shift reflects the Philippines' determination to secure its interests and achieve its national goals.

However, these developments drew a sharp rebuke from China. Beijing's fictitious 10-dash line combined with its allegation that the Philippines is being used as a pawn by the United States remains a standard counter narrative. Meanwhile, its aggressive actions in the WPS also coincide with a surge in disinformation activities and cyberattacks. This can be seen in various counter narratives aimed at presenting an alternative reality and undermine the Philippine claim. In parallel, several cyberattacks against government agencies were experienced during the same period. The author believes that this is part of a convergence of offensive cyber and disinformation activities that is consistent with Beijing's gray zone playbook.

At this juncture, we need to understand how this threat convergence strategy is pursued and identify the necessary actions that can frustrate its goals. The Philippines cannot afford to be passive-reactive in confronting such an elaborate campaign. Given the current political developments, adversaries can easily use cyber-enabled disinformation combined with offensive cyber capabilities to further push its malign influence agenda.

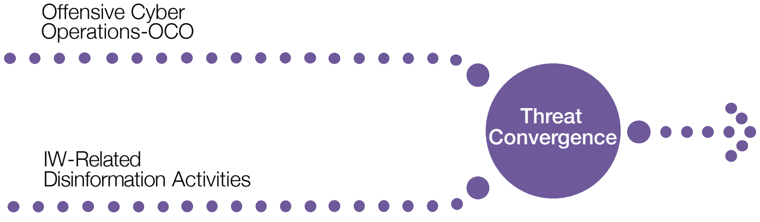
The Weaponization of Cyberspace and Information

Traditionally, the weaponization of information relies on the ability of an actor (or actors) to manipulate and use it as a resource for military or strategic gain. It can also inhibit an adversary from accessing the resource, thus degrading its decision-making capabilities, and fomenting confusion among others (Whyte et al, 2021). This ability is usually referred to as information warfare (IW). IW is defined as follows:

> *"The integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting its own." (US DOD, 2012)*

However, Russian influence operations in Ukraine in 2014 and its alleged involvement in the 2016 United States presidential elections, expands IW beyond its military domain. Suddenly, the traditional view of IW evolved into a broader strategy that aims to influence citizen perception as part of gray zone and asymmetric warfare (Whyte et al, 2021). Moreover, this new IW use-case exploits the ubiquitous nature of the Internet and the dependence on digital technologies, paving the way for its weaponization (Gomez, 2021; Whyte et al, 2021). Suddenly, the optimism brought about by the benefits of openness, collaboration, and innovation has been tainted by anxiety and insecurity. Another facet of this evolving attempt to weaponize cyberspace is the ability to mount offensive cyber operations (OCOs) combined with IW practices like disinformation and psychological operations. These activities are intended to disrupt an adversary's digital infrastructure through hacking, denial of service attacks, data theft among others (Whyte & Mazanec, 2019). Moreover, the internet has become a venue to launch digital attacks and spread disinformation. Malicious actors have become diverse, ranging from state-sponsored hackers, terrorists, and criminal organizations. This convergence of OCO and IW-related disinformation activities points to an ominous goal of weakening the foundations of truth and knowledge, while impairing the decision-making capabilities of an adversary (Figure 1). It can also rapture societal fault lines and introduce doubt in the decision-making process, with the aim of manipulating data and sentiment (Foote et al., 2021). Furthermore, Libicki (2021) argues that the appeal of this threat convergence emanates from the enhancing effect of offensive cyber capabilities to psychological operations. This is partly due to the shift in the consumption of traditional news media to less curated websites and uncurated social media content, which permits its rapid spread.

Figure 1 . Convergence of OCO and IW-Related Disinformation



Source: Author's Data Management

Foreign Malign Influence Operations

Another aspect of the weaponization of cyberspace is its use in the current geopolitical competition. In this scenario, countries seek to influence an adversary's internal political system through unofficial means, using deception and other opaque techniques to achieve its desired outcomes (Searight, 2020). In general, foreign malign influence (FMI) operations aim to disrupt decision-making, weaken partnerships, erode trust and foment divisions in society, ultimately undermine its institutions (Ingram, 2020). Furthermore, FMI is often seen in the active spread of disinformation that targets the vital sectors of society, especially its political and economic spheres (DHS, 2019). Table 1 shows the various technologies and techniques used in FMI operations.

Possible Goals of the Threat Convergence

- *Disruption of services*
- *Degrade and adversary's decision-making capabilities*
- *Foment distrust, confusion, and sow discord*
- *Undermine institutions and values of an adversary*

Table 1 . New Technologies and Techniques Used in Foreign Malign Influence (FMI) Operations

- **False Information Operations**- This refers to the spread of false information through traditional and social media. It aims to weaponize information to manipulate and mislead the population.
- **Deep Fake Technologies**- This AI-enabled technique allows malign actors to manipulate video that will allow for manipulation of digital content and false attribution. Advanced mimicking software can also imitate human characteristics that can be used by malign actors to deceive a target audience.
- **Deep Video Portrait**- Like deep fakes, this technique preserves the live action actor and manipulates the actor's environment. Also, it does not involve face swapping, but has the capability to manipulate facial movements.
- **Cyber Warfare**- This refers to attacks against critical infrastructure through digital means. The intent is to disable or disrupt a service or function. Theft of intellectual property and cyber espionage is also part of this domain.
- **Financial Influence**- This technique is about transferring money into a country to fund malign influence operations.
- **Backing of Extreme Political Groups**- The act of providing financial and logistical support to adversaries/malign actors operating within a political boundary or country.

Source: Department of Homeland Security, 2019

In addition, FMI allows malign actors to exploit the vulnerabilities of the internet and the low-cost of offensive cyber tools. Innovations in artificial intelligence (AI) can add another ominous side to this emerging environment. Radsch (2022) explains that these campaigns will exploit the vulnerabilities in social media platforms and use AI to pursue a digital manipulation strategy. This approach can undermine legitimate news by drowning it with fake news and the use of deep fakes intended to manipulate public opinion.

China's Views on Information Warfare

Since the 1990s, Beijing has viewed the digital information space as a venue for strategic competition and has allotted the resources to dominate it. Harold et al. (2021) describes the PRC's information operations as elaborate, well-coordinated, and sufficiently funded. For its information operations, it is allegedly being run through a well-organized structure overseen by its United Front as part of propaganda. A key outcome in the agenda is the "disintegration of enemy forces" through its 3-warfares (3Ws) approach (Box 1).

For its part, the People's Liberation Army (PLA) has transformed itself into a highly informatized, cyber-enabled armed force capable of operating in a digitally connected battlefield (Pollpeter et al., 2017). Also, the PLA's information

Box 1 . The PLA's 3-Warfares Approach

- *Strategic Psychological Operations: The pre-conflict posturing of military/paramilitary forces or application of other national capabilities (diplomatic, economic, cultural) with the intention of intimidating adversaries and encouraging acquiescence to PRC-desired outcomes*
- *Overt and Covert Media Manipulations: The use of materials delivered to public audiences through established news services, informal internet sites, and other social media to influence domestic and international perspectives associated with ongoing disputes involving the PRC's interests.*
- *Exploitation of National and International Legal Systems: The leveraging of existing legal regimes and processes to constrain adversary behavior, contest disadvantageous circumstances, confuse legal precedent, and maximize advantage in situations related to the PRC's core interests.*

Source: Livermore 2018

and cyber capabilities are part of its strategic deterrence posture together with its nuclear and space forces (Kania, 2021). This view is anchored on the primacy of non-kinetic techniques that aim to diminish its adversary's will to fight. It is also seen as a force multiplier that complements its political and diplomatic efforts (Ibid). Furthermore, this concept is also part of China's intent to establish information dominance in both peacetime and during armed conflict. In fact, the PLA's Central Military Commission has promulgated official guidelines through its departments for the integration of 3Ws in doctrines development and training (Kania, 2021).

At present the 3Ws approach is employed as part of its gray zone strategy (Livermore, 2018). Its strategic psychological operations are intended to use its national power (i.e., Economic, Political, and Military) to intimidate or seek the acquiescence of adversaries by shaping both local and international discourse (Zhang et al, 2023). While covert and overt media operations aim to use traditional and social media as well as informal venues to influence a target audience. The third facet is the exploitation of national and international legal systems where it aims to constrain its adversaries and confuse legal precedence (Livermore, 2018). This emphasis on information is also reflected in how the PLA conducts its operations on social media. Hsini and Tien-Shen (2018) enumerated the three types of disinformation operations namely: (a) target of opportunity attacks; (b) steady-state disinformation campaigns and (c) long term campaigns anchored on creating narratives.

Operationalizing the 3-Warfare Approach (3Ws): Learning from the Taiwan experience

Actual cases can provide important insights of how the 3Ws concept is operationalized. The Taiwanese experience offers firsthand account of the ferocity of these attacks. Purportedly instigated by the PRC, the case shows the use of offensive cyber operations combined with a cyber enabled disinformation campaign. For instance, during the 2020 presidential elections, it has been reported that it has experienced 20-40 million attacks per month (Kania, 2021). Similarly, during the visit of high-profile United States officials in 2022, its government reported an astonishing 50 million attacks per day (60 minutes, 2022). The 3Ws approach was extensively used to manipulate public opinion during the 2018 election and in Beijing's joint invasion scenarios of the island. The campaign seeks to undermine the will of the Taiwanese people to resist and foment division in public opinion (Kania, 2021; DoubleThink Labs, 2022).

Another prominent example is the 2020 presidential elections wherein PRC-initiated disinformation operations are seen as uniquely decentralized and dispersed. It utilized social media platforms for its influence operations by spreading pro-unification and anti-Democratic Progressive Party (DPP) content (Zhang, 2020). Aside from Facebook and Twitter, YouTube was another favored platform for disinformation activities due to its popularity. Furthermore, the campaign also used troll farms and AI-generated content using local accents (DoubleThink Labs, 2022). The aim of these activities is to create a semblance of popular support for its unification message. Table 2 presents several instances of alleged PRC-enabled disinformation activities:

Table 2 . Additional Examples of Disinformation Activities in Taiwan

- A PTT report that the Taiwanese consulate in Japan failed to evacuate it citizens during the height of Typhoon Jebi in September of 2018. The report stated that Taiwanese citizens were evacuated by the PRC, claiming that they are their brothers and sisters. This created a huge public backlash in Taiwan, which resulted in the suicide of the head of its diplomatic office in Osaka, Japan. The report later turned out to be false.
- The use of the popular Taiwanese messaging app, LINE, to spread misinformation about the Tsai government. A false report about the suspension of pensions for citizens traveling without authorization was spread through the app.
- These activities also exploit issues that are controversial and tend to have diverse public opinions. LGBTQ rights and pension reform are examples of these concerns.

Source: Zhang, 2020 (DoubleThink Labs, 2022)

In the run up to the 2024 elections, reports of cyberattacks and a surge in disinformation activities remain a common occurrence. For instance, Meta reports that it has cracked down on Chinese influence operations by closing 7,500 accounts across its platforms. While Chinese propaganda has made known of its preference of the Kuomintang (KMT) party. This is often expressed through the narrative that the result of the national elections is a choice between war and peace (Kelter, 2023). In addition, rumors about the shipment of poisoned pork from the U.S. and the claim that Taiwan has surrendered its rights when it shifted electronic chip manufacturing overseas were mainstreamed. Apparently, this is part of an elaborate plot to weaken the relationship between Taiwan and the U.S. (Wong, 2024). Another characteristic of this insidious act is the coopting of Taiwanese citizens through economic incentives (termed as investments), usually through donations to online channels and individuals. It also uses overt marketing campaigns to propagate Beijing's interests and the messages are often mixed with entertainment to mask its intent (Shen, 2022).

These ominous events clearly show that Taiwan is a target of cyber coercion intended to spread fear, panic, and confusion with the purpose of intimidating its people (Manantan, 2020). Allegedly perpetrated by the PRC, the weaponization of cyberspace has become a hallmark for asymmetric and gray zone warfare not only in Taiwan, but in Southeast Asia as a whole (Curtis, 2020). These insidious acts are intended to undermine its democratic institutions and in Taiwan's case, prepare for a possible invasion.

The Hong Kong Experience

The experiences of Hong Kong during the 2019 pro-democracy protest adds another important facet to the convergence of offensive cyber and cyber-enabled disinformation. Mass actions triggered by proposed laws that limit the territory's autonomy are clearly illustrated in Beijing's offensive cyber and disinformation capabilities. Taking a page from the Russian playbook, the spread of disinformation throughout popular social media sites like Facebook and Twitter was intended to achieve a desired political outcome by controlling the narrative. In addition, messaging through YouTube seem to amplify the violent and destructive nature of the pro-democracy movement (Conger, 2019). An example of this post is an attempt to dehumanize the protesters by comparing them to ISIS terrorists, dogs, and cockroaches (Matsakis, 2019).

These malicious activities forced Facebook and Twitter to take appropriate actions. In fact, Twitter reports that it has deleted 936 accounts while YouTube disabled 210 channels that are allegedly linked to the PRC (Paul & Culliford, 2019). In addition, cyberattacks occurred in parallel with disinformation activities. The protest movement used social media and popular messaging apps like Telegram and WhatsApp to organize and communicate. However, these same tools were hacked to dox protesters' identities, sending a chilling effect among members of the movement (Kuo, 2019). For instance, during the June 2019 protest actions against China's extradition law, popular messaging app Telegram was hacked, causing the denial of its service. Telegram was a popular messaging tool for protesters due to its end-to-end security encryption. This feature is supposed to prevent spying on online communications (Shanapinda, 2019). Due to the leak, several organizers of the platform were arrested by Hong Kong authorities. Telegram would later trace the DDOS attack against its servers to China (Nauman, 2019). The doxing of activists also resulted in cyberbullying, which targeted the leadership of the movement with acts ranging from intimidation, sexual harassment, and death threats (Adams & Lytvynenko, 2019).

Signs of Things to Come: The Philippine Experience

The Philippines is not exempt from the dangers of FMI. For instance, Cambridge Analytica whistleblower Christopher Wylie said that they regard the Philippines as a "petri dish" for disinformation techniques. He further states that the country was a good testing ground since it meets three underlying conditions, namely: (1) High social media usage, (2) Questionable rule of law, and (3) Corrupt politicians. The country's weak regulatory infrastructure and high social media usage has made it possible for Cambridge Analytica to test out these strategies before deploying them in Western economies (Occeñola, 2019). In addition, Wylie also revealed that around 87 million Facebook users' data was harvested and targeted for political campaigns. Of these numbers, 1.2 million users came from the Philippines, the second highest after the United States (Ibid).

Another powerful account of the country's vulnerability to disinformation is evidenced by the efforts of Facebook and Instagram to eliminate fake accounts in 2019. Known as Operation Naval Grazing, an estimated 155 accounts, 11 pages, 9 groups, and 6 Instagram accounts were removed for violating the platform's policy against foreign or government interference. The perpetrators stole pictures from individuals and used AI-generated profile pictures to disguise the fake accounts. These accounts the posed as citizens from Southeast Asia posted messages in support of the Chinese narratives in the South China Sea. These pages also echoed anti-U.S. sentiments and has supported politicians who are sympathetic to Beijing (Nimmo et al., 2020).

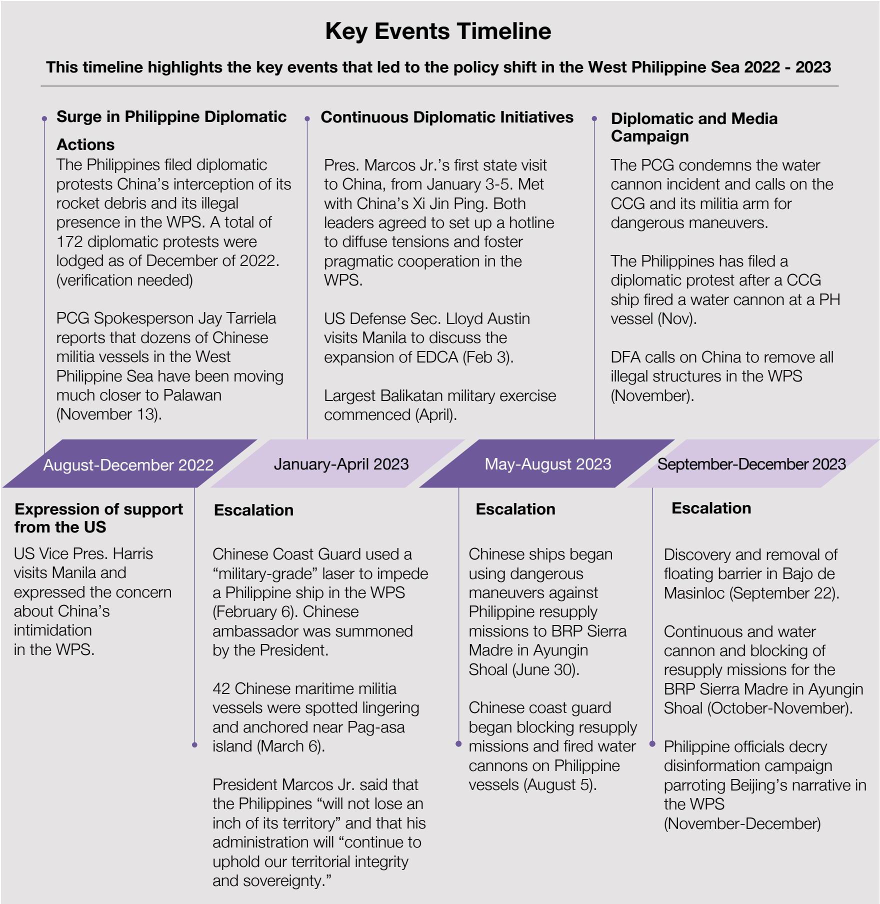
In addition, Chalk (2023) cites that the disinformation activities are part of Beijing's foreign influence operations which have the following goals: (a) Sow discord in the Philippines and encourage the population to focus on internal conflicts and issues; (b) Weaken Manila's partnerships and alliances with its allies, in particular the U.S.; and (c) Shape the public opinion to support Beijing's position in the SCS. For instance, in a September 2023 Senate inquiry, PCG spokesperson Commodore Jay Tarriela has confirmed that journalists supporting government efforts in the WPS have received emails intended to divert attention to issues concerning Vietnam. Nonetheless, Commodore Tarriela did not confirm if such emails directly came from China but said that such kind of coordinated information operations could only have been sponsored by a state actor (CNN Philippines, 2023). Similarly, according to a report by the Philippine Center for Investigative Journalism (PCIJ), there is a small community of Filipinos that are actively pushing Beijing's narratives. Among them include supposed think tanks like the Integrated Development Studies Institute (IDSI) and the Asian Century Philippines Strategic Studies Institute (ACPSSI) (Elemia, 2023). For the IDSI, the report suggested that the growing escalation in the WPS as a "mind conditioning or future false flag to bring the United States war to Asia after Ukraine," clearly pushing Beijing's narrative. Meanwhile, the ACPSSI have said that the water cannon incident was "benign" and a mere "spray" further stating that for 24 years, deliveries to the BRP Sierra Madre have "always been successful,". These claims are meant to downplay the recent blocking and reckless maneuvers by Chinese vessels (One News PH, 2023; Elemia, 2023).

Nonetheless, national security officials have said that there are no clear indications that pro-Beijing narratives are gaining any traction. However, they have warned that if these narratives are not exposed or corrected, there is fear that public opinion could be swayed due to the country's high social media usage and vulnerability to disinformation.

The Philippine Situation in the West Philippine Sea and the Role of Malign Influence

The statement that the Philippines "will not relinquish an inch of its territory" given by President Ferdinand Marcos Jr. expressed the government's strong commitment to defend its sovereignty and uphold its rights under UNCLOS. This declaration is a contrast from his earlier stand that the Philippines will be "a friend to everyone and an enemy to none". This shift can be attributed to the aggressive and illegal activities of the CCG and its militia arm in the WPS. Furthermore, these provocative acts also resulted in a pivot towards its traditional Western allies like the United States, Japan, Canada, and Australia, among others. This renewed relationship is mainly focused on strengthening security and economic cooperation as well as deepening diplomatic engagements (Manhit, 2023). In Figure 2, notable examples of this pivot can be seen in the visit of Vice President

Figure 2 . Timeline of Events



Key Events Timeline

This timeline highlights the key events that led to the policy shift in the West Philippine Sea 2022 - 2023

Surge in Philippine Diplomatic Actions

The Philippines filed diplomatic protests China's interception of its rocket debris and its illegal presence in the WPS. A total of 172 diplomatic protests were lodged as of December of 2022. (verification needed)

PCG Spokesperson Jay Tarriela reports that dozens of Chinese militia vessels in the West Philippine Sea have been moving much closer to Palawan (November 13).

Continuous Diplomatic Initiatives

Pres. Marcos Jr.'s first state visit to China, from January 3-5. Met with China's Xi Jin Ping. Both leaders agreed to set up a hotline to diffuse tensions and foster pragmatic cooperation in the WPS.

US Defense Sec. Lloyd Austin visits Manila to discuss the expansion of EDCA (Feb 3).

Largest Balikatan military exercise commenced (April).

Diplomatic and Media Campaign

The PCG condemns the water cannon incident and calls on the CCG and its militia arm for dangerous maneuvers.

The Philippines has filed a diplomatic protest after a CCG ship fired a water cannon at a PH vessel (Nov).

DFA calls on China to remove all illegal structures in the WPS (November).

August-December 2022

January-April 2023

May-August 2023

September-December 2023

Expression of support from the US

US Vice Pres. Harris visits Manila and expressed the concern about China's intimidation in the WPS.

Escalation

Chinese Coast Guard used a "military-grade" laser to impede a Philippine ship in the WPS (February 6). Chinese ambassador was summoned by the President.

42 Chinese maritime militia vessels were spotted lingering and anchored near Pag-asa island (March 6).

President Marcos Jr. said that the Philippines "will not lose an inch of its territory" and that his administration will "continue to uphold our territorial integrity and sovereignty."

Escalation

Chinese ships began using dangerous maneuvers against Philippine resupply missions to BRP Sierra Madre in Ayungin Shoal (June 30).

Chinese coast guard began blocking resupply missions and fired water cannons on Philippine vessels (August 5).

Escalation

Discovery and removal of floating barrier in Bajo de Masinloc (September 22).

Continuous and water cannon and blocking of resupply missions for the BRP Sierra Madre in Ayungin Shoal (October-November).

Philippine officials decry disinformation campaign parroting Beijing's narrative in the WPS (November-December)

Source: Author's Data Management

Kamala Harris in November of 2022, where she assured the Philippines that the United States will be a strong ally in the face of intimidation and coercion in its waters. She also decried how foreign illegal fishing, depletion of fish stock, and harassment as well as the intimidation of local fisherfolks has had a significant effect on coastal communities (Lema, 2022). This was followed by a visit from Defense Secretary Lloyd Austin in February 2023 where he expressed the "iron-clad" commitment of the United States to defend the Philippines as part of its Mutual Defense Treaty. Secretary Austin together with then-Department of National Defense Senior Secretary Carlito Galvez also announced the inclusion of additional military bases for the Enhanced Defense Cooperation Agreement (EDCA) and the holding of several Balikatan exercises for 2023.

In addition, the state visit of Japanese Prime Minister Fumio Kashida in November of 2023 underscored the need for both countries to renew its security and economic ties. It was reported that PM Kashida and Pres. Marcos discussed the proposed Reciprocal Access Agreement between the two countries. This agreement will provide the framework that will allow military forces of the two nations to have access to bases and to conduct regular exercises.

In the following months after the visit of VP Harris, dozens of Chinese militia vessels were spotted moving much closer to Palawan. The Department of Foreign Affairs (DFA) filed diplomatic protests over illegal fishing and the unauthorized presence of these vessels as well as its harassment of local fisherfolk. Meanwhile, the PCG has been continuously challenging these militia vessels but has not received any response (Mangosing, 2022).

To improve bilateral relations, President Marcos traveled to China for an official visit on January 3-5, 2023. With the intent of reinvigorating the country's economic relationship with its northern neighbor, the visit was overshadowed by the WPS issue. In addition, a direct communications channel was agreed to be set up between the two countries' foreign ministries and that their respective coast guards would meet and discuss pragmatic cooperation (Yew & Morales, 2023). Later, the PCG announced that it has abandoned the hotline (CNN Philippines, 2023).

In March of 2023, Chinese incursions were on the rise. Subsequent reports indicate that 42 Chinese maritime militia vessels were spotted lingering and anchored near Pag-asa Island. PCG personnel were then directed to document all their activities and to forward it to the DFA for appropriate action (Manabat, 2023). In July 2023, the menacing activities of the Chinese Coast Guard (CCG) and its militia arm increased significantly. The CCG began deploying military grade lasers, conduct blocking maneuvers and the use of water cannon to harass Philippine supply vessels bound for the BRP Sierra Madre in Ayungin Shoal. This culminated in the ramming and the water cannoning incident in November of 2023 involving a civilian resupply vessel carrying AFP Chief of Staff Gen. Romeo Brawner.

An Emerging Convergence of Offensive Cyber and Disinformation Activities

a. Offensive Cyber and disinformation incidents

While the intimidation activities of the CCG and its militia arm were in full swing, it is quite noticeable that the Philippines experienced simultaneous offensive cyber and disinformation activities. Table 3 provides examples of these incidents during the period of January to December of 2023.

Table 3 . Offensive Cyber And Disinformation Activities Along with Escalation Incidents in the WPS for Period January-December 2023

Period 2023	**Escalation Incidents**	**Cyber and Disinformation Activities**
Period 1 January-April	• February 6: Chinese Coast Guard used a “military-grade” laser to impede a Philippine ship in the WPS. • February 14: Chinese ambassador was summoned by President Marcos for the first time. • March 6: 42 Chinese maritime militia vessels were spotted lingering and anchored near Pag-asa Island.	**Disinformation** • February 6: Pro-China posts echoed claims of Chinese state media that additional military bases for EDCA make the Philippines a “pawn” in the impending US-China war over Taiwan (Macaraeg, 2023). **Cyber attacks** • April 19: PNP and NBI report data breach affecting 1.2 million records. This coincides with the largest Balikatan military exercise between the PHL and the US (Acosta, 2023).
Period 2 May-August	• June 30: Chinese ships began using dangerous maneuvers against Philippine resupply missions to BRP Sierra Madre in Ayungin Shoal.	**Disinformation** • August: Social media posts downplayed China’s actions (firing of water cannon) and attempts to dismiss

Source: Authors’ Data Management

Table 3 . Offensive Cyber And Disinformation Activities Along with Escalation Incidents in the WPS for Period January-December 2023

Period 2023	Escalation Incidents	Cyber and Disinformation Activities
	• August 5: Chinese coast guard began blocking resupply missions and fired water cannons on Philippine vessels.	China's harassment were also present. A post from a prominent columnist claimed that the Philippine government supposedly promised to remove BRP Sierra Madre from Ayungin Shoal (Macaraeg, 2023). • August 9: Think tank Integrated Development Studies Institute (IDSI) pushed pro-Beijing narratives by suggesting that the escalation in the SCS was a "mind conditioning or future false flag to bring US war to Asia after Ukraine" (Elemia, 2023). • August 10-14: Anonymous accounts on X (formerly Twitter) flooded WPS discourse accusing PCG Spokesperson Jay Tarriela of being a "CIA agent" working for the US government and a "traitor" for selling intelligence services (Chi, 2023). • August 16: Manila-based think tank Asian Century Philippines Strategic Studies Institute (ACPSSI) defended China's use of water cannon on national television, calling it "benign" and a mere "spray." Further stating that for 24 years, that deliveries to BRP Sierra Madre "has always been successful," downplaying the recent blocking and reckless maneuvers by Chinese vessels (One News PH, 2023). **Cyber-attack** • August 20: Attempts to hack the emails of phones of government officials belonging to the National Task Force for the West Philippine Sea (Carvajal, 2023).
Period 3 September-December	• September 22: Discovery and removal of floating barrier in Bajo de Masinloc. • October-November: Continuous and water cannon and blocking of resupply missions for the BRP Sierra Madre. • November-December: Philippine officials decry disinformation campaign parroting Beijing's narrative in the WPS.	**Disinformation** • September 12: PCG Spokesperson Jay Tarriela said that journalists supporting the PH government's efforts in the WPS have received emails trying to divert attention and focus of the Filipino people, trying to divert attention away from the WPS (CNN Philippines, 2023). • September 25: Global Times, effectively the mouthpiece of the Chinese Communist Party posted an article which quoted an expert saying the Philippines is

Source: Authors' Data Management

Table 3 . Offensive Cyber And Disinformation Activities Along with Escalation Incidents in the WPS for Period January-December 2023

Period 2023	Escalation Incidents	Cyber and Disinformation Activities
		acting under the influence of Washington, who's bent on instigating conflicts in the region in order to contain China (The Straits Times, 2023). • October 16: China accuses the Philippines of violating its sovereignty, illegally occupying an island in the WPS (CNA, 2023). • October 23: NSC publicly recognized the existence of China's "operators" or "proxies" undermining PH's claims in the WPS; think tanks echoing and pushing Beijing narratives in social media platforms and press conferences (IDSI & ACPSSI) (Elemia, 2023). • November 28: Fake and altered images were uploaded on Youtube saying that the Philippine Coast Guard had begun firing water cannons at Chinese vessels (Terong Explained, 2023). • December 10: The Philippine Coast Guard said China had again used water cannons on resupply and coast guard vessels and intentionally rammed into them. This is contrary to the disinformation Chinese official statements are saying that it was the Philippine vessel that intentionally rammed into the Chinese coast guard ship (Al Jazeera, 2023). • December 27: ACPSSI said in an interview in CGTN that the Philippines is being used as a "pawn" of the United States, and that the latter has exerted so much influence in the latter's foreign policy (CGTN, 2023). **Cyber-attack** • September 22: PhilHealth reports ransomware attack affecting 20-million member records. Hackers demanded for US 300,000 as ransom (Jaymalin, 2023). • October 10: Philippine Statistics uthority reports a hacking incident affecting its CBMS repository (Ronda, 2023). • October 12: House of Representatives reports that their website was defaced (Cabato, 2023).

Source: Authors' Data Management

In April of 2023, the Philippine National Police (PNP) and the National Bureau of Investigation (NBI) reported a massive data breach affecting sensitive documents. Aside from data from NBI clearances, records from the PNP's Special Action Force were also affected. Similarly, the Bureau of Internal Revenue and the Civil Service Commission reported comparable incidents (Acosta, 2023). These occurrences seem to coincide with the April 2023 Philippine-US Balikatan military exercise, which was announced as the largest in its history.

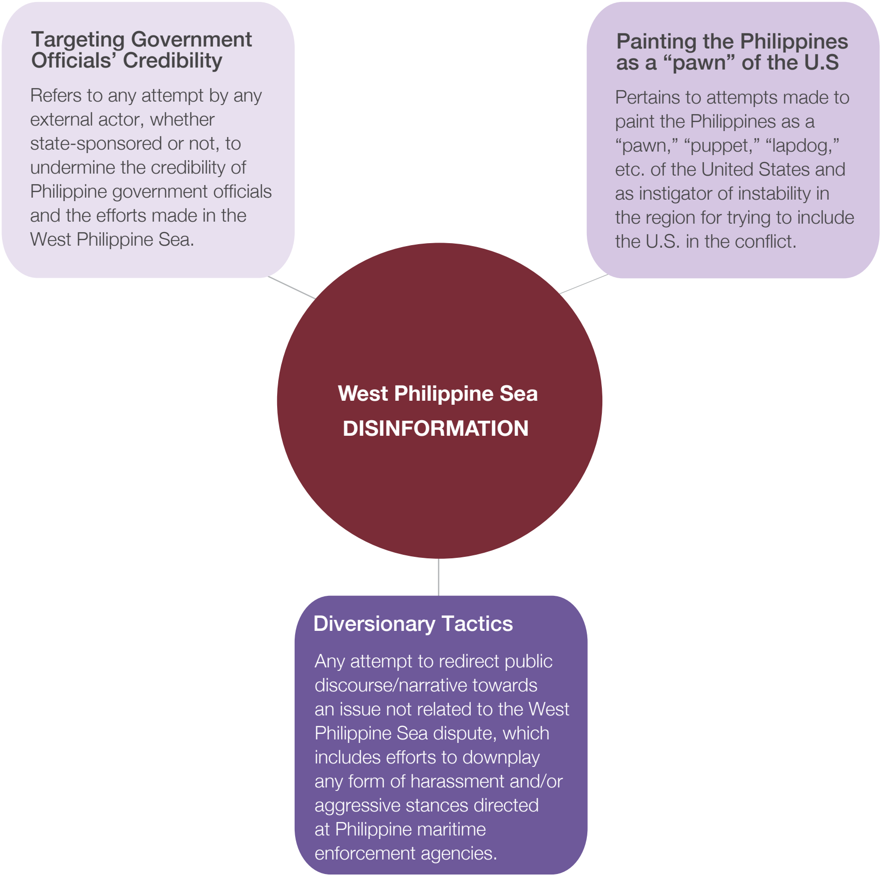
The removal of the floating barriers from Bajo de Masinloc (September 2023) and the subsequent water cannon incidents as well as the blockade of the Ayungin shoal (October-November 2023) also coincided with malicious cyber events. In particular, the PhilHealth ransomware attack and the hacking of the systems of the Philippine Statistical Authority occurred in September of 2023. Meanwhile, the House of Representatives also stated that their website was defaced the following month (Jaymalin, 2023; Ronda, 2023). In a press statement, the Department of Information and Communications Technology (DICT) Secretary Ivan Uy acknowledged that there were several other government agencies that were affected but opted not to report the incident.

In the same month, several media sites reported that executives of the National Task Force for the West Philippine Sea have experienced digital attacks targeting their phones and emails. It was not mentioned however, which specific country or entity these attacks came from, but it is important to take note that these attacks came at a time of heightened tensions in the WPS (Carvajal, 2023).

b. Emerging Disinformation Themes

The emerging cyber-enabled disinformation activities can be classified into three recurring themes. First, activities targeting the credibility of Philippine government officials. This is part of a playbook in which a malign external actor (state or non-state) attempts to undermine the credibility of its adversary. Second, there were instances where diversionary tactics were used to redirect public discourse and consciousness away from to the WPS dispute. For instance, there were moves to downplay the harassment of PCG ships and redirect the issue to the current situation in Vietnam (CNN Philippines, 2023). Finally, there were persistent claims portraying the Philippines as a lackey of the United States (i.e. "Pawn," "puppet," and "lapdog,"). The Philippines was accused of causing instability in the region by attempting to involve the United States and

Figure 3 . Recurring Messaging Themes about the WPS



Targeting Government Officials' Credibility

Refers to any attempt by any external actor, whether state-sponsored or not, to undermine the credibility of Philippine government officials and the efforts made in the West Philippine Sea.

Painting the Philippines as a "pawn" of the U.S

Pertains to attempts made to paint the Philippines as a "pawn," "puppet," "lapdog," etc. of the United States and as instigator of instability in the region for trying to include the U.S. in the conflict.

West Philippine Sea DISINFORMATION

Diversionary Tactics

Any attempt to redirect public discourse/narrative towards an issue not related to the West Philippine Sea dispute, which includes efforts to downplay any form of harassment and/or aggressive stances directed at Philippine maritime enforcement agencies.

Source: Author's Data Management

other nations in the conflict. Figure 3 summarizes the emerging disinformation themes.

In addition, Table 4 provides examples of opposing claims circulating on various social media platforms and their respective engagement numbers. It should be noted that these samples are not exhaustive, but they illustrate a possible disinformation campaign surrounding the WPS issue.

Several pro-China messages were posted on Facebook during the first quarter of 2023, criticizing the Philippines for being too dependent on the United

Table 4 . Examples of Opposing Claims and Counter Narratives Using Social Media Platforms

Disinformation Post	**Date Posted**	**Engagements** (as of January 2024)
Facebook: Post from a newspaper columnist suggesting that giving Americans additional access to PH bases places the PH in harm's way vis-à-vis issues in Taiwan.	February 6, 2023	249 reactions, 308 comments, and 109 shares
X (formerly Twitter): A Filipino vlogger said that the Philippines is being "sucked" into the SCS "maelstrom." Further says that the US is behind this manipulative agenda.	August 7, 2023	69.6 thousand views, 275 shares, 950 likes, and 60 bookmarks
Facebook:A Manila based think-tank suggested that the escalation in the SCS was a "mind conditioning or future false flag to bring the US war to Asia after Ukraine"	August 9, 2023	24 reactions, 13 comments, and 8 shares
X (formerly Twitter): A verified account is suggesting that PCG Spokesperson Jay Tarriela is a "CIA agent."	August 10, 2023	Three separate posts with 137; 1,903; and 1,108 views.
Facebook: Post accusing PCG Spokesperson Jay Tarriela is "unpatriotic," a "traitor," and accepts bribes from the US in the form of favors.	August 14, 2023	193 reactions, 16 comments, and 36 shares.
YouTube: Manila-based think tank Asian Century PAnother Manila-based think tank defended China's use of water cannon on national television, calling it "benign" and a mere "spray." " It further stated that for 24 years, that deliveries to BRP Sierra Madre "has always been successful," downplaying the recent blocking and reckless maneuvers by Chinese vessels.	August 16, 2023	19 thousand views and 210 likes
YouTube: Fake and altered images were uploaded on YouTube saying that the Philippine Coast Guard had begun firing water cannons at Chinese vessels.	November 28, 2023	122,516 views and 2.8 thousand likes

Source: Authors' Data Management

States. These posts also downplayed the blatant harassment and incursions by the CCG and its militia arm (Macaraeg, 2023). In an interview, local pro-Beijing commentators argued that the Philippines is being used as a "pawn" of the United States and accused the latter of undue influence on Philippine foreign policy (CGTN, 2023). Moreover, two prominent Facebook users (with 47,000 and 203,000 followers) reiterated the same narrative and cautioned that the Philippines is being drawn into a deeper conflict. One of the said posts had garnered 249 likes with 109 shares. Similarly, the IDSI posted drone footage from the Chinese Coast Guard on Facebook that suggests downplaying the water cannon firing that occurred in August 2023.

In addition, PCG spokesperson Commodore Jay Tarriela has been a consistent target of disinformation on both Facebook and X (formerly Twitter). In August 2023, several posts on X suggested that Commodore Tarriela is a "CIA agent" and was selling intelligence services to the United States. The posts also resurrected controversies surrounding his cadetship at the Philippine Military Academy (Chi, 2023). On a Facebook post which had garnered 193 likes and 36 shares, Tarriela was accused of being unpatriotic and a traitor for receiving bribes in the form of certificates and "pocket money." (Macaraeg, 2023)

Aside from Facebook and X, YouTube is another popular platform for pushing Beijing's narratives. For instance, pro-Beijing commentators downplayed China's aggressive actions had gained 19000 views and 193 likes. Meanwhile, a video uploaded by the channel Terong Explained, falsely claimed that the PCG had fired back at the Chinese vessels. The video has been viewed over 122,000 times and has received more than 2,800 likes. The channel has about 464,000 subscribers.

Nonetheless, even with its obvious timing and messaging, attribution of cyber and disinformation activities remains a challenge. Harold et al. (2021) cites the lack of evidence establishing Chinese involvement in disinformation activities in the WPS. However, the authors argued that it does not necessarily mean that China is not active in one way or another. The US-China Economic and Security Commission cites four UNFWD affiliated groups – China Council for the Promotion of Peaceful National Reunification (CCPPNR), Chinese People's Association of Friendship with Foreign Countries (CPAFFC), China Overseas Friendship Association (COFA), and the China Zhi Gong Party (CZGP) as as alleged conduits for spreading disinformation. Moreover, Chinese influence in traditional media has also become apparent as they have been accused of echoing pro-Beijing sentiments while maintaining strong ties with pro-China organizations in the country (Harold et al., 2021).

Official Chinese Pronouncements on the WPS Issue

In general, social media posts from malign actors are in line with the official statements from the Chinese Foreign Ministry and its official news outlets. These pronouncements often dismiss and downplay the reckless and aggressive tactics against the Philippines. On February 13, Wang Wenbin, spokesperson for the Chinese Foreign Ministry, challenged reports claiming that the CCG had recklessly blocked Philippine resupply missions to Ayungin Shoal. He failed to mention the 'military-grade' laser pointing incident that was carried out by the CCG (PRC Foreign Ministry, 2023). Wang further said that the CCG only responded in a "professional and restrained way."

In another incident on October 22, Beijing released a statement downplaying the collision, referring to it as "slight" one. It also said that the CCG was "lawfully" blocking the Philippine ship from transporting "illegal construction materials" intended for Ayungin Shoal (Santos, 2023). Days later, the Chinese Embassy in Manila released an official statement that the escalating tensions in the West Philippine Sea has been "inflated" by the United States (Cupin, 2023).

In a similar incident on December 10, China accused a Philippine ship of making an "unprofessional and dangerous sudden turn, intentionally ramming" into a CCG vessel. The CCG even called on the Philippines to stop its "provocative acts," further saying that Beijing would continue its law enforcement activities in the WPS. However, PCG Commodore Tarriela, armed with video footage, refuted such claims, saying that it was the CCG vessel that rammed and fired its water cannon at the Philippine vessel (Al Jazeera, 2023). In another instance, the Chinese Foreign Ministry seemingly mocked the Philippine government for removing the floating barriers near Bajo de Masinloc, saying it "looks nothing more than self-amusement" (Santos, 2023).

Guarding Against Malign Influence

With Beijing's intention to establish information dominance to achieve its goals in the SCS, it will certainly use all resources at its disposal to achieve its desired outcomes. Therefore, the Philippines must examine its vulnerabilities and find ways to mitigate its effects. Our ability to use a conceptual lens is also vital to enable a collective action approach.

For this reason, Filipino officials and planners can use the FMI concept to examine the current environment. Here, we can benefit from our knowledge of how Beijing and its cohorts subscribe to the 3Ws philosophy (Strategic Psychological Operations, Covert & Overt Media Campaigns, and Exploitation of the International-National Legal Systems). This insight can provide us with how its various agencies and the People's Liberation Army (PLA) operationalize FMI. Another valuable insight is the convergence of offensive cyber and disinformation activities. In the WPS issue, this precarious combination exploited the vulnerabilities of government institutions and the pervasiveness of social media in the country. These allowed malign actors to easily spread false narratives about the WPS and portray the Philippine government as incompetent and a pawn of the West. Listed below are the possible vulnerabilities that can be exploited by FMI actors:

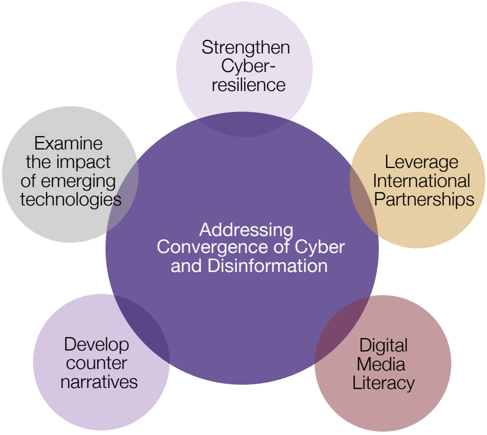
- The WPS situation as a low priority issue among Filipinos: Although there seems to be a consensus about its importance, the recent Pulse Asia survey reveals that only six percent of Filipinos consider the WPS conflict as important. This also means that malign actors will use other priority issues to shift the public's consciousness away from the WPS issue.
- Malign influence actors are always on the lookout for opportunities to sow division, undermine their adversary and foment chaos. A country's political and governance spheres are obvious targets for these activities. For instance, the current feud between the Marcos Administration and the Duterte camp is an opportunity for malign actors to divide the country and shift the public's attention away from the WPS. An example of this is the viral video on YouTube about the "polvoron issue" accusing Pres. Marcos of being a drug addict as well as the alleged destabilization plots. For FMI operators, these are opportunities that can be exploited by shifting the attention of citizens away from the WPS issue while undermining the credibility of the current government.
- FMI operations often exploit the weaknesses of a democratic society. The democratic values of protecting freedoms of speech and the press as well as elections are possible targets for these malicious actors. For instance, several studies cite Beijing's attempt to control Taiwanese media

through acquisition of news outfits and coopting of digital content creators. The purpose of this effort is to support the unification narrative with the mainland and dissuade calls for independence. The Philippines can learn from the Taiwan experience. The country's midterm elections in 2025 can be a venue for FMI operators to use their techniques to undermine its credibility.

Recommendations: Address Convergence of Offensive Cyber and Disinformation Activities

Filipino officials and planners must recognize that the convergence of offensive cyber operations and disinformation activities is a new and menacing threat. As part of a gray zone playbook, this dangerous combination will ultimately be part of a foreign malign influence agenda aimed at weakening the Philippine position in the WPS. For this reason, the country's strategy to deal with this threat should veer away from its traditional fragmented and siloed approach. Instead, a proactive and long-term plan based on the concepts of cyber defense, psychological operations, and information warfare is needed. Figure 4 shows the possible components of this strategy, followed by a discussion on each section.

Figure 4 . Components of a Strategy to Address Cyber Convergence and Foreign Malign Influence (FMI)


Strengthen Cyber-resilience
Examine the impact of emerging technologies
Leverage International Partnerships
Addressing Convergence of Cyber and Disinformation
Develop counter narratives
Digital Media Literacy

Source: Author's Data Management

Enumerated below are the possible components of this strategy:

a. *Strengthen cyber resilience*- This component calls for a deliberate effort to identify the country's critical sectors and determine their readiness as well as vulnerabilities against offensive cyber and disinformation campaigns. Programs aimed at capacitating individuals and organizations are key activities. For instance, initiatives that will allow critical sectors to establish standards on digital maturity, risk assessment, and business continuity are crucial aspects of attaining resilience. Also, the ability to share and collaborate on cyber threat assessment and mitigation is another important part of this component.

b. *Digital media and information literacy*- Literacy programs on new media and information security are also essential in attaining a proactive stance against disinformation and malign influence. This component includes a media campaign that will foster awareness about the threats of FMI operations. In addition, this component also underscores the role of traditional and social media outfits in promoting trustworthy news and clamping down on fake news. Civil society organizations and the academe among others can also contribute through fact-checking and meaningful research.

c. *Leverage international cooperation*- One of the strongest qualities of the Philippine position in the WPS is its adherence to international law and the rules-based order. Because of this, the country has gained the sympathy and support of many nations. The Philippines can also learn from the experiences of various countries and governments. This will provide us with a deeper understanding of our adversary's playbook.

d. *Develop compelling counter narratives*- Aside from viewing the WPS as an issue of sovereignty and maritime security, another facet that should be leveraged is how the conflict is adversely affecting the country's blue economy. This will result in a broader conversation that includes non-traditional issues such as environmental protection, maritime safety, the livelihood of fisherfolk communities among others. This will allow the Philippines to control the narrative and gain a moral high ground, thus appealing to a wider audience. For instance, Chinese aggression can be presented not only as blatant disregard of a rules-based order but also result in huge environmental consequences and disproportionate impact on the livelihood of Filipino fisherfolks.

e. *Examine the possible impact of emerging technologies*- Lastly, Filipino officials and planners should examine the developments in AI and quantum computing. These technologies hold tremendous potential in health, business, and government. However, malign actors are cognizant of its usefulness in FMI operations. For instance, AI-enabled deep fakes and mimicking apps combined with big data analytics can provide malicious agents with powerful tools for espionage, disinformation, and cybercrime.

In summary, the convergence of offensive cyber operations and disinformation activities against nations sets a dangerous trend for malign influence operations. If perpetrated by states, these activities pose a serious threat to societal cohesion and shared values among countries. Unfortunately, the Philippines is at the frontline of this fight. The strong position of the Marcos government in the WPS issue has also resulted in a surge in malicious cyber activities. It will not be surprising to see this threat convergence as part of FMI operations against our country.

Therefore, it is crucial for the country to adopt a proactive and strategic approach in mitigating these threats. Fortunately, the Philippines is not alone. Its adherence to truth, transparency, and a rules-based approach in the WPS has enabled the country to gain the support and assistance of its international partners. More importantly, with the right policies and programs, the country can count on the resilience of its people to overcome these emerging challenges.

REFERENCES

60 Minutes. (2022). China's Cyber Assualt on Taiwan. Retrieved from https://www.youtube.com/watch?v=Agc3vy-JD4c

Acosta, R. (2023). Cybersecurity firm reports leak of 'sensitive' PNP, NBI other government agencies' documents in breach. Businessmirror. Retrieved from https://businessmirror.com.ph/2023/04/20/cybersecurity-firm-reports-leak-of-sensitive-pnp-nbi-other-government-agencies-documents-in-breach/

Adams, R., & Lytvynenko, J. (2019). Someone Is Doxing Hong Kong Protesters And Journalists — And China Wants Them To Keep Going. Buzz New Feeds. Retrieved from https://www.buzzfeednews.com/article/rosalindadams/hong-kong-doxing-protesters-china-encourage

Al Jazeera. (2023, December 23). Philippines and China accuse each other of South China Sea collisions. (A. J. AGENCIES, Producer) Retrieved 2023, from https://www.aljazeera.com/news/2023/12/10/philippines-and-china-accuse-each-other-of-south-china-sea-collisions

CGTN. (2023, December 27). Philippine scholar: U.S. is using the Philippines as a pawn. CGTN. Retrieved from https://news.cgtn.com/news/2023-12-27/Philippine-scholar-U-S-is-using-the-Philippines-as-a-pawn-1pSwkcmG91e/p.html

Chalk, P. (2023, May 19). PRC Influence Operations in the Philippines: Can Beijing Flip the South China Sea Script? The Jamestown Foundation. Retrieved December 2023, from PRC Influence Operations in the Philippines: Can Beijing Flip the South China Sea Script?

Chi, C. (2023). Anonymous accounts flood WPS discourse with 'CIA agent' accusations vs PCG spox. News Article. Retrieved December 2023, from https://www.philstar.com/headlines/2023/12/04/2316405/anonymous-accounts-flood-wps-discourse-cia-agent-accusations-vs-pcg-spox

CNA. (2023, October 16). China says Philippines violated its sovereignty, illegally occupied island in disputed waters. CNA-Mediacorp. Retrieved December 2023, from https://www.youtube.com/watch?v=J_g7KKEziJs

CNN Philippines Staff. (2023, August 12). Hotline between PH, China coast guards now defunct – PCG. CNN Phils. Retrieved December 2023, from https://www.cnnphilippines.com/news/2023/8/12/pcg-ccg-hotline-now-defunct.html#google_vignette

CNN Philippines Staff. (2023, September 12). PCG: Possible China-sponsored disinformation campaign on WPS underway. CNN Phils. Retrieved December 2023, from https://www.cnnphilippines.com/news/2023/9/12/pcg-possible-wps-disinformation-campaign-underway.html

Conger, K. (2019, August 20). Hong Kong: China is spreading disinformation about pro-democracy protests, Facebook and Twitter say. Independent-Asia Edition. Retrieved January 2024, from https://www.independent.co.uk/news/world/asia/hong-kong-protests-latest-china-disinformation-facebook-twitter-social-media-a9071046.html

Cupin, B. (2023, October 26). Days after Ayungin collision, China Embassy in Manila says US 'inflating' tensions. Manila, Philippines: Rappler. Retrieved December 2023, from https://www.rappler.com/philippines/china-embassy-manila-statement-blames-united-states-inflating-tensions-october-2023/

Curtis, J. (2021). Springing the 'Tacitus Trap': countering Chinese state-sponsred disinformation. SMALL WARS & INSURGENCIES , 229-265.

DHS. (2019, May 21). HOMELAND SECURITY ADVISORY COUNCIL INTERIM REPORT OF THE COUNTERING FOREIGN INFLUENCE SUBCOMMITTEE. Department of Homeland Security.

DOD. (2012). Joint Publication 3-13 on Information Operations. US Department of National Defense.

DoubleThink Labs. (2021). Deafening Whispers: China's Information Operation and Taiwan's 2020 Election. Taipei, Taiwan: DoubleThink Lab. Retrieved December 2023, from https://medium.com/doublethinklab/deafening-whispers-f9b1d773f6cd

Elemia, C. (2023, October 23). Philippines confronts unlikely adversary in SCS row: Filipinos echoing 'pro-Beijing' narratives. Manila, Philippines: Phil. Center for Investigative Journalism. Retrieved December 2023, from https://pcij.org/article/10888/philippines-confronts-unlikely-adversary-south-china-sea-row-filipinos-echo-pro-beijing-narratives

Foote, C., & Maness, R. J. (2021). Cyber conflict at the intersection of information operations. In C. Whyte, T. Thrall, & B. Mazanec, INformation Warfare in the Age of Cyber Conflict (pp. 54-70). Routledge.

Gomez, M. (2021). Cyber-emabled information warfare and influence operations. In C. Whyte, T. Thrall, & B. Mazanec, INformation Warfare in the Age of Cyber Conflict (pp. 132-145). Routledge.

HAROLD, S., BEAUCHAMP-MUSTAFAGA, N., & HORNUNG, J. (2021). Chinese Disinformation Efforts in Social Media. Santa Monica, CA, USA: RAND Corporation.

Ingram, H. (2020, February 20). The Strategic Logic of State and Non-State Malign Inluence Activities. The RUSI Journal, 12-24.

Kelter, F. (2023, December 23). How Beijing is changing the way it involves itself in Taiwan's election. Retrieved December 2023, from https://www.msn.com/en-us/news/world/how-beijing-is-changing-the-way-it-involves-itself-in-taiwan-s-election/ar-AA1lHNor

Kuo, L. (2019, June 14). Hong Kong's digital battle: tech that helped protesters now used against them. The Guardian. Retrieved January 2024, from https://www.theguardian.com/world/2019/jun/14/hong-kongs-digital-battle-technology-that-helped-protesters-now-used-against-them

Lazaro, J., & Santos, T. (2023, September 29). China spokesperson mocks PH removal of shoal barrier as 'self-amusement'. Phil. Daily Inquirer. Retrieved January 2024, from https://globalnation.inquirer.net/220049/china-spokesperson-mocks-ph-removal-of-shoal-barrier-as-self-amusement

Lema, K. (2022, November 23). U.S. stands with Philippines against coercion in South China Sea - Harris. Reuters. Retrieved December 2023, from https://www.reuters.com/world/us-vp-harris-visits-philippine-island-edge-contested-south-china-sea-2022-11-22/

Libicki, M. (2021). The convergence of information warfare. In C. Whyte, T. Thrall, & B. Mazanec, Information warfare in the age of cyber conflict (pp. 15-26). Oxon, UK: Routledge.

Livermore, D. (2018, March 25). China's "Three Warfares" In Theory and Practice in the South China Sea. Georgetown University Center for Security Studies. Retrieved December 2023, from https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/

Macareg, P. (2023, November 1). How Chinese propaganda is seeded online in the Philippines. Rappler. Retrieved January 2024, from https://www.rappler.com/newsbreak/investigative/ways-how-china-propaganda-seeded-online-philippines/

Manabat, J. (2023, March 06). 42 Chinese vessels linger near Pag-asa Island. ABS CBN News. Retrieved January 2024, from https://news.abs-cbn.com/news/03/06/23/42-chinese-ships-linger-near-pag-asa-island

Manantan, J. (2020). The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the SCS. Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs, 1-29.

Mangosing, F. (2022, December 07). Chinese militia vessels coming closer to Palawan. Phil. Daily Inquirer. Retrieved January 2023, from https://globalnation.inquirer.net/208965/chinese-militia-vessels-coming-closer-to-palawan

Manhit, V. (2023, March 20). Philippine President Marcos Jr.'s Foreign Policy Emphasizes Cooperation. Bower Group-Asia. Retrieved December 2023, from https://bowergroupasia.com/philippine-president-marcos-jr-s-foreign-policy-emphasizes-cooperation/

Matsakis. (2019, August 19). China Attacks Hong Kong Protesters With Fake Social Posts. Wired. Retrieved January 2024, from https://www.wired.com/story/china-twitter-facebook-hong-kong-protests-disinformation/#:~:text=In%20response%20to%20widespread%20pro-democracy%20demonstrations%20in%20Hong,disclosures%20made%20by%20Twitter%20and%20Facebook%20on%20Monday.

Nauman, Q. (2019, June 13). Telegram traces cyber-attack during HK protests to China. Phys.Org. Retrieved January 2024, from https://phys.org/news/2019-06-telegram-cyber-attack-ceo-hk-protests.html

Newsweek. (2024, January 18). China Raises Private Hacker Army To Probe Foreign Governments. Retrieved January 26, 2024, from https://www.newsweek.com/china-hackers-probe-foreign-governments-computers-online-cybersecurity-1861721

Nimmo, B., Eib, S., & Ronzaud, L. (2020). Operation Naval Grazing: Facebook takes down inauthentic Chinese netwroks. Graphika. Retrieved December 2023, from https://graphika.com/reports/operation-naval-gazing

One News PH. (2023, August 16). Manila-based think tank defends China's water cannon attack. Retrieved from https://www.youtube.com/watch?v=pvOaT_cR7LE

Paul, K., & Culliford, E. (2019, August 20). Twitter, Facebook accuse China of using fake accounts to undermine Hong Kong protests. Reuters. Retrieved January 2024, from https://www.reuters.com/article/us-hongkong-protests-twitter-idUSKCN1V91NX/

Pollpeter, K., Chase, M., & Heginbotham, E. (2017). The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations. RAND Corporation. Retrieved January 2024, from https://www.rand.org/pubs/research_reports/RR2058.html

PRC Ministry of Foreign Affairs. (2023, Feburary 12). Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference. Retrieved January 2024, from . https://www.mfa.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202302/t20230213_11024546.html

Radsch, C. (2022). ARTIFICIAL INTELLIGENCE AND DISINFORMATION: STATE-ALIGNED INFORMATION OPERATIONS AND THE DISTORTION OF THE PUBLIC SPHERE. Vienna: Office of the Organization for Security and Co-operation in Europe. Retrieved December 2023, from https://www.osce.org/files/f/documents/e/b/522166.pdf

Searight, A. (2020, May 8). Countering China's Influence Operations: Lessons from Australia. Center for Strategic and International Studies. Retrieved December 2023, from https://www.csis.org/analysis/countering-chinas-influence-operations-lessons-australia

Shanapinda, S. (2019, June 14). How a cyber attack hampered Hong Kong protesters. Retrieved from PHYS.ORG: https://phys.org/news/2019-06-cyber-hampered-hong-kong-protesters.html

Shen, P. (2022). How China Initiates Information Operations. Taipei, Taiwan.

Stockton, J., & Wiley, N. (2022). Battling Malign Influence in the Open: Open source intelligence addresses global threats. Signal. Retrieved December 2023, from https://www.afcea.org/signal-media

Terong Explained. (2023, November 28). NAKU PO LAGOT KAYO! PH Coast Guard GUMAMIT NA Ng Water Cannon Sa WEST PH SEA! Retrieved December 2023, from https://www.youtube.com/watch?v=zrQWOcQ8mhc

The Strait Times. (2023, September 26). China tells the Philippines not to 'stir up trouble' over disputed shoal. Retrieved January 2024, from https://www.straitstimes.com/asia/philippines-says-china-has-removed-remnants-of-floating-barrier-in-south-china-sea

Tian, Y. L., & Morales, N. (2023, January 5). China, Philippines agree to handle disputes peacefully, boost cooperation. Reuters. Retrieved January 2024, from https://www.reuters.com/world/asia-pacific/china-philippines-agree-direct-communication-channel-south-china-sea-2023-01-05/

Twigg, K., & Allen, K. (2021, March 12). The disinformation tactics used by China. British Broadcasting Corporation. Retrieved January 2024, from https://www.bbc.com/news/56364952

Whyte, C., & Mazanec, B. (2019). Understadning Cyber Warfare: Politics, Policy and Strategy. New York: Routledge.

Whyte, C., & Mazanec, B. (2019). Unerstanding Cyber Warfare. Devon, UK: Routledge.

Zhang, A., Hoja, T., & Latimore, J. (2023). Gaming Public Opinion: The CCP's increasingly sophisticated cyber-enabled influence operations. Australian Strategic Policy Institute.

Zhang, L. (2020, September-October). How to counter China's disinformation campaign in Taiwan. Military Review.

ACKNOWLEDGMENTS

The Stratbase ADR Institute extends its deepest gratitude to all involved in developing this special study. This publication would not have been possible without your commitment, collaboration, and support.

The strength of this special study comes not from any single policy. Rather, it draws from the collective insight of our expert authors from the academe, public and private sectors, and civil society. Hence, we are grateful for our authors' generous sharing of knowledge and experiences that make up this special study.

We would especially like to thank Prof. Victor Andres 'Dindo' Manhit, President of the Stratbase ADR Institute, for this initiative would never have come to fruition without his leadership, vision, and direction.

Finally, we would like to thank the tireless and dedicated members of the Stratbase ADR Institute;

Our design consultant, Ms. Carol Manhit, for the publication layout and cover design;

Stratbase ADR Institute's editorial team composed of Deputy Executive Director for Research, Dr. Jimmy Jimenez, Deputy Executive Director for Programs and External Affairs, Ms. Krystyna Louise C. Dy, Research Director Venice Isabelle Rañosa, and Director for Policy and Advocacy Ms. Shanice Espiritu-Amador for their diligence and hard work.

ABOUT THE AUTHOR

Sherwin E. Ona, Ph.D
Non-resident Fellow
Stratbase Albert Del Rosario Institute

Dr. Ona is an associate professor and the chairperson of the Department of Political Science and Development Studies of the De La Salle University-Manila (DLSU). Previously, Dr. Ona was the former research and advanced studies director of the College of Computer Studies of the DLSU. His research interests include the areas of open government, digitalization, human security, cybersecurity policies, and disaster informatics.

For his research endeavors, Dr. Ona was part of the iGov summer program of the State University of New York from 2009 to 2010 and he also managed the e-Participation in rural communities project supported by the International Development Research Cooperation-Canada (IDRC) in 2011. In 2012, he was part of the IDRC's "Open Data in Developing Countries", a global network of international research teams that examined the challenges of open government data in developing and least developed economies. In 2017, Dr. Ona served as a senior team leader for the Newton disaster informatics and innovation spaces project sponsored by the British Council and the Commission on Higher Education (CHED).

Dr. Ona also served as a technical consultant to several government agencies and international organizations including the Commission on Information and Communications Technology in 2005, the Department of Science and Technology-ICTO in 2012, the Commission on Higher Education in 2017, and the Department of Information and Communications Technology in 2018. In 2019, he was appointed as a consultant of the United Nations-Asia Pacific Center for Information and Communication Technology for Development (APCICT) on Data Governance and Interoperability.

Dr. Ona is a senior fellow of the Philippine Public Safety College and the and the La Salle Institute of Governance. He is also an auxiliary officer of the Philippine Coast Guard with the rank of commander.

The views, opinions and conclusions expressed in this paper are those of the author and do not necessarily reflect those of the Institute or any of its officers and trustees.

The author is solely responsible for its content.

stratbase +ADRi PUBLICATIONS
STRATBASE ADRi FOR STRATEGIC AND INTERNATIONAL STUDIES

The Financial Tower
6794 Ayala Avenue
Makati City,
Philippines 1226

www.adrinstitute.org