Discussion Paper Series 2025

STRATEGIC STUDIES PROGRAM

In Technology We Trust?

The Struggle to Build a Cyber Force in the Philippines

Francis C. Domingo

STRATEGIC STUDIES PROGRAM

In Technology We Trust?

The Struggle to Build a Cyber Force in the Philippines

Francis C. Domingo

UP CIDS Discussion Paper Series
is published by the

University of the Philippines
Center for Integrative and Development Studies
Lower Ground Floor, Ang Bahay ng Alumni
Magsaysay Avenue, University of the Philippines
Diliman, Quezon City 1101

Telephone: (02) 8981-8500 loc. 4266 to 4268 / (02) 8426-0955
Email: cidspublications@up.edu.ph
Website: cids.up.edu.ph

cids.up.edu.ph

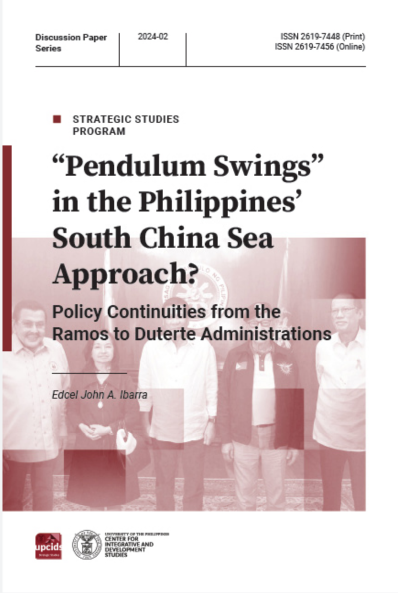
The views and opinions expressed in this discussion paper are those of the author/s and neither reflect nor represent those of the University of the Philippines or the UP Center for Integrative and Development Studies. No copies can be made in part or in whole without prior written permission from the authors/editors and the publisher.

ISSN 2619-7448 (Print)
ISSN 2619-7456 (Online)

Cover image credit
"Soldiers Military Cyber Warfare with Digital Battlefield Overlay - Global Cyber Security."

KaihkoImages. AI Generated. Adobe Stock. https://stock.adobe.com/ph/images/soldiers-military-cyber-warfare-with-digital-battlefield-overlay-global-cyber-security/952852899

Table of Contents



Discussion Paper Series | 2024-02 | ISSN 2619-7448 (Print)
ISSN 2619-7456 (Online)

STRATEGIC STUDIES PROGRAM

“Pendulum Swings” in the Philippines’ South China Sea Approach?

Policy Continuities from the Ramos to Duterte Administrations

Edcel John A. Ibarra

UNIVERSITY OF THE PHILIPPINES
CENTER FOR INTEGRATIVE AND DEVELOPMENT STUDIES

UNIVERSITY OF THE PHILIPPINES
CENTER FOR INTEGRATIVE AND DEVELOPMENT STUDIES

ISSN 2619-7278 (Print)
ISSN 2619-7286 (Online)

Policy Brief
2024-04

STRATEGIC STUDIES PROGRAM

Defending the West Philippine Sea

Japan's Crucial Role in Countering Gray Zone Operations in the Maritime Domain

Jikko Alfonso Puzon[1]

During the commemorative summit for the 50th anniversary of the ASEAN-Japan Friendship and Cooperation, President Ferdinand Marcos Jr. was asked in a media interview to share his thoughts on the current approach of the Philippines in dealing with its maritime dispute with China. While he has remained open to the possibility of working with President Xi Jinping through peaceful dialogue and consultations, President Marcos Jr. said that his administration's diplomatic efforts with China have shown no signs of progress. He admitted that traditional methods of diplomacy, such as a démarche or a diplomatic protest, have not been effective (Mangaluz and Lazaro 2023).

President Marcos Jr. then stressed the crucial need for a paradigm shift as tensions in the maritime domain continue to rise. He said the situation with China is heading in a poor direction and would remain the same if the Philippines does not change its ways (Mangaluz and Lazaro 2023). In line with this, President Marcos Jr. urged the Philippine government "to move the needle" and develop a new concept or approach to maintaining peace and stability in the West Philippine Sea.

Under his leadership, cracks in the country's relations with China have become more noticeable. While he has consistently advocated for the peaceful resolution of disputes, China has intensified its coercive and illegal activities in the maritime domain. Aside from its construction and militarization of artificial islands in various parts of the West Philippine Sea, it has also deployed its coast guard and maritime militia to intimidate and harass Philippine vessels in the disputed waters.

On December 6, 2023, the House of Representatives (HOR) adopted House Resolution No. 1494 to condemn China's aggression in the West Philippine Sea (Cervantes 2023a). The resolution described in detail China's coercive and illegal activities in the maritime domain, including its dangerous maneuvers against Philippine Coast Guard (PCG) vessels, harassment of Filipino fishermen in Bajo de Masinloc (Scarborough Shoal), and

[1] Jikko Alfonso Puzon (jikkoalfonso.puzon@gmail.com) is a Filipino researcher and a former Visiting Research Fellow at The Japan Institute of International Affairs (JIIA).

IN TECHNOLOGY WE TRUST?

The Struggle to Build a Cyber Force in the Philippines

Francis C. Domingo

Associate Professor
Department of Political Science
University of the Philippines Diliman

Research Fellow
Strategic Studies Program
UP Center for Integrative and Development Studies

fcdomingo2@upd.edu.ph

HIGHLIGHTS

- The paper explores the strategic challenges that confront the Armed Forces of the Philippines' development of a cyber force.

- The paper argues that the military's struggle to build a cyber force is influenced by three domestic factors: limited appreciation of cyber power, bureaucratic politics, and insular nature of Philippine strategic culture.

- The military's limited appreciation of cyber power can contribute to misleading beliefs about the strategic utility of cyber capabilities and contribute to threat inflation.

- Bureaucratic politics among government agencies can make it difficult for a cyber force to perform its functions due to disagreements over mandate in cyber engagements, as well as the prioritization of their institutional self-interests.

- The insular nature of Philippine strategic culture can affect the development of a cyber force because it can shape the preference of the military to prioritize the use of cyber capabilities for internal security operations.

INTRODUCTION

Cyberspace has evolved as a strategic domain for cooperation and conflict among states. Powerful states have exploited the permanent dependence on cyber-enabled technologies to strengthen the global economy while covertly advancing their national security interests using cyber operations. Military forces are one of the few government organizations authorized to develop and maintain capabilities for conducting cyber effect operations against adversaries. The steady increase in the development of military cyber organizations or *cyber forces* around the world suggests that hostile actions in cyberspace are now part of the new normal in geopolitics.[1] Indeed, the number of states that developed cyber forces increased from four states in 2000 to sixty-one states in 2018, with the largest number of cyber forces located in Western Europe and North America (Blessings 2020; Smeets 2023). Existing studies on military innovation and cyber strategy mention at least four factors that influence the development of cyber forces.

The first factor relates to organizational considerations that may affect the development of a cyber force. States are confronted with substantial constraints in adapting to the cyber domain, mainly because of issues related to "organizational structure, operational mandate, and the availability of skills and resources" (Smeets 2023). A related point is enhancing organizational efficiency and effectiveness. States such as Estonia, Germany, and Norway created cyber forces with the objective of integrating, consolidating, and streamlining formerly fragmented Information and Communication Technologies (ICT) as well as cyber-related capabilities and organizations. This potentially "eliminates overlapping roles and responsibilities, and [enables a] more efficient use of resources in the context of limited defense spending in many countries" (Pernik 2020, 189).

[1] "Cyber forces are active-duty military organizations that possess the capability and authority to direct and control strategic computer network operations in the cyber domain to impact, change, or modify strategic diplomatic and military interactions between entities," (Blessings 2020).

The second factor, strategic culture, relates to another internal consideration that affects the development of cyber forces.[2] Strategic culture is a crucial factor in influencing how states use cyber power to advance their national interests. For instance, recent studies argue that strategic culture is useful in explaining how states cope with the uncertainty in cyberspace. Specifically, "strategic culture exists as a cognitive schema that mediates the interpretation of strategic realities and shapes preferences in pursuit of strategic goals" (Gomez 2021, 34). Another study argues that a *technology-oriented* strategic culture is a necessary condition for the development of cyber capabilities in small states. Moreover, strategic beliefs and practices are a "filtering mechanism" that shapes the responses of small states to imbalance distribution of capabilities in cyberspace (Domingo 2022).

The third factor relates to external considerations, particularly the role of threats and material resources. External security concerns over increasing cyber capabilities among adversaries combined with material constraints (e.g. funding) drive the development of cyber force. The insecurity due to perceived advantages of cyber capabilities influenced states like China and the United States to lead the development of a cyber force ahead of most states in the international system (Gomez 2016; Craig and Valeriano 2018; Blessings 2020).

The fourth factor relates to another external consideration, the role of alliances. In the alliance between Japan and the United States, the state with cyber capacity helps the partner-country to develop its own capacity, increasing the alliance's overall security and reducing mutual vulnerabilities in cyberspace. Partner-countries that lack cyber capacity are eager to accept help from states with cyber force because it is more efficient than developing cyber capacity from zero (Kallender and Hughes 2016; Smith and Ingram 2017; Kostyuk 2024).

This paper draws on the literature on cyber strategy and policy and analyzes the factors that constrain the development of a cyber force in the Philippines. While other states are preparing to deploy its cyber forces, the Philippines is

[2] Strategic culture can be defined as a "distinctive body of beliefs, attitudes and practices regarding the use of force, which are held by a collective (usually a nation) and arise gradually over time, through a unique protracted historical process" (Longhurst 2004, 17).

still trying to make sense of how cyber power can be employed strategically to shape its diplomatic and military interactions. The increasing number of cyber intrusions against government agencies in the past three years has intensified discussions about creating a cyber force; however, a confluence of factors has impeded progress in the military's attempt to build a cyber force (Crismundo 2023; Rosales 2023; Domingo 2024). In this context, this paper explores the prospects of developing a cyber force from a strategic perspective. It argues that the military's struggle to build a cyber force is influenced by three internal factors: limited appreciation of cyber power, bureaucratic politics, and insular nature of Philippine strategic culture. The paper explores this argument by drawing on recently published government documents, existing work on the sources of military strategy in the Philippines as well as the emerging academic literature on military operations in cyberspace.[3]

Although scholars and analysts have written on cyber issues in the Philippines, studies on cyber issues are mostly technical and do not engage with the debates on military innovation and cyber strategy. The remaining parts of the paper proceed in six sections to primarily address this issue. The next section discusses the concepts, functional stages, and characteristics of military cyber operations. The third explicates how limited appreciation of cyber power in the military obscures the creation of a cyber force. The fourth section examines how bureaucratic politics complicates the coordination between government agencies responsible for countering state-sponsored cyber intrusions. The fifth section traces how the insular nature of Philippine strategic culture impedes the development of a cyber force. The sixth section offers some considerations that can address the challenges identified. The last section synthesizes the main points of the paper.

[3] The research on military operations in cyberspace is relatively new, with most of the studies published in the past five years. See for example Gomez (2016), Blessings (2020), Brantly and Smeets (2020), Pernik (2020), Lindsay (2021), Smeets (2022, 2023), Kostyuk (2024).

CONCEPTUALIZING MILITARY CYBER OPERATIONS

Military cyber operations are increasingly mentioned in media and technical reports, but these activities are often misrepresented as *cyber weapon*s or *cyber attacks*. Military cyber operations are defined as engagements designed to achieve strategic, operational, and tactical outcomes using computer systems and networks that "damage or harm to living or material entities" of adversarial states (Smeets 2017; Brantly and Smeets 2020).

There are three types of cyber operations conducted by military forces: computer network attack, computer network defense, and computer network exploitation. Computer network attack or offensive operations involve the disruption, denial, degradation, and destruction of information in computers and information systems. Computer network defense or defensive operations involve the detection, analysis, and mitigation of threats and vulnerabilities posed by adversaries. Computer network exploitation or espionage involves the collection of intelligence on other states and adversaries through cyberspace (U.S. Department of Defense 2010).

The conduct of cyber operations consists of several stages depending on the type and objective of the operation. While several frameworks have been created to explain how cyber operations are executed, Lockheed Martin's Cyber Kill Chain framework is adopted since it is more appropriate for the scope and substance of the paper.[4] The Cyber Kill Chain is composed of seven stages of cyber operations as summarized in Table 1. The first stage, reconnaissance, involves conducting research to determine which targets will allow them to meet their objectives. The second stage, weaponization, relates to the development of payload (i.e. malicious software), the identifying the entry point (i.e. backdoor implant), as well as an appropriate command and control infrastructure for the operation.

[4] Lockheed Martin developed the framework based on the traditional military concept of *kill chain* or the process of planning and launching an attack. A prominent alternative to Cyber Kill Chain is MITRE attack. This framework is more technical in nature because it focuses more on the intricacies of tactics, techniques, and procedures involved in cyber intrusions. See for example Korolov and Myers (2022).

The third stage, delivery, refers to the deployment of the malicious software to the target through controlled (against web servers) or released (malicious email). The fourth stage, exploitation, involves gaining access to the target's computer systems by exploiting software, hardware, or human vulnerabilities. The fifth stage, installation, relates to insertion of a persistent backdoor or implant in the target's environment to maintain access for an extended period. The fifth stage, command and control, concerns the establishment of a command channel to enable remote manipulation. The sixth and final stage, actions on objectives, involves carrying out the original objectives such as data exfiltration (espionage), violations of data integrity (subversion), or disabling computer systems and networks (sabotage) (Hutchins, Cloppert, and Amin 2011).

TABLE 1. STAGES OF A CYBER OPERATION

(BRADLY AND SMEETS 2020, 4)

STAGE	DESCRIPTION
Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload
Delivery	Transmission of weapon to target
Exploitation	Once delivered, the weapon's code is triggered; exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command and Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network
Actions on Objectives	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Military operations in cyberspace are distinctive compared to other domains because of four characteristics: nonphysical, stealth, functional, and pervasive. The first, military cyber operations are nonphysical. These operations do not directly cause physical damage or harm. The primary instruments used in cyber operations are cyber weapons or malicious computer codes that are not tangible. However, they can still cause kinetic damage. This fundamental characteristic defines the nonphysical nature of computer network operations as well as the possible strategic outcomes that cyber operations can achieve.

The second characteristic is stealth. The deployment of cyber weapons is difficult to detect because malicious software can pretend to be legitimate. They can also be integrated within legitimate computer programs that seem to be non-threatening to users. The stealthy nature of cyber operations is further illustrated by the challenge of attributing cyber incidents. Attributing cyber intrusions is difficult because it requires time and resources particularly when adversaries use “multi-stage attacks, where the attacker infiltrates one computer to use as a platform to attack a second, and so on” (Clark and Landau 2011, 27). This method, when applied across multiple jurisdictions, increases the barriers for discovery thereby making attribution complicated to achieve.

The third characteristic is functionality or the range of actions that can be undertaken to support military operations. Cyber operations are functional because these capabilities can enable different military strategies across different domains of warfare (McGuffin and Mitchell 2014). More specifically, these capabilities contribute to military operations by performing three functions: defensive operations, offensive operations, and espionage. A fundamental function of military cyber operations is defense or proactively protecting computer networks from intrusion by adversaries. Another function is offense, which involves disrupting or shutting down the command-and-control systems of adversaries in support of military operations. The last function is exploitation or collecting intelligence through computer networks. Exploitation and offensive cyber operations follow similar stages of operations, but espionage is a more difficult task because it is “tougher to penetrate a network and reside on it undetected while extracting large volumes of data from it than it is to, digitally speaking, kick in the front door and fry a circuit or two…” (Hayden 2016, 137 cited in Brantly and Smeets 2020).

The fourth characteristic is the pervasiveness. Operations in cyberspace can support military operations in other environments simultaneously and effectively without exhausting resources. While military power employed through land, sea, air, and space can generate strategic effect across different domains, these dimensions of military power cannot sustain concurrent operations because of the risk of resource depletion (Sheldon 2019). The pervasive reach of cyber operations is manifested in the significance of cyber technologies in all sectors of society.

LIMITED APPRECIATION OF CYBER POWER

Cyber power is "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain" (Nye 2011, 123). There are limited examples of cyber power being used in actual military combat, and the veracity of accounts in these isolated cases is subject to debate. For military planners, it is the strategic use of cyber power that is of significant interest. Since cyber power is used to achieve definable objectives as part of an overall strategy, limited appreciation of its utility impedes military forces from developing the capacity to operate in cyberspace (Sheldon 2019).

The advantages of using cyber power have been extensively discussed in previous studies. For example, Gray (2013) emphasizes the non-physicality of cyber power. "Cyber power is not like other kinds of military power; all of the others have physical reality and can engage physically with the rest," (p. 36) Rattray (2009) highlights functionality, "Cyber power 'has become a fundamental enabler for the full range of instruments of national power: political, diplomatic, economic, military, and informational,"(p. 255). Meanwhile, Sheldon (2019, 298) focuses on stealth— the "ability to stealthily use cyber power, aided by the inherent difficulties of attributing the identity and motivation of most attackers, makes it a very attractive instrument for governments and other actors."

Despite these advantages, the use of cyber power as a strategic instrument continues to be underappreciated in the Philippines. The discourse relating to cyber threats in the past decade focuses on criminal activities and protection of critical infrastructure with little mention of cyber conflict and state-sponsored cyber intrusions. This predicament is clearly reflected in the different strategies published by the government: national security strategy, the national defense strategy, and the national military strategy.

The National Security Strategy (NSS) of the Philippines was released in 2018. The NSS was created "to foster better coordination, synchronization, and cohesion of government functions in order to improve efficiency and maximize the use of limited State resources." (National Security Council [NSC] 2018, 26–29).The document highlights the effective use of the national instruments of power. The NSS mentions the *informational, technological,* and *military* instruments of power, but there is no discussion on how these instruments can be utilized strategically against adversaries (National Security Council [NSC] 2018, 26–29). The NSS considers cyber issues as an *urgent national security concern*, however, the priorities articulated in the document mostly refer to technical (e.g. common criteria program) and law enforcement (e.g. countering web-based crime) issues (NSC 2018, 65–66). Indeed, the most sophisticated cyber threats—espionage, sabotage, and subversion—are not discussed in the NSS, making it difficult to understand the military's role in securing cyberspace, as well as the overall strategic utility of cyber power for the state.

The National Defense Strategy 2018—2022 (NDS) raises expectations regarding the use cyber power as a strategic instrument because cyber security is identified as a strategic priority by the defense and military communities (Department of National Defense [DND] 2018, 17). The NDS was released in 2019 and was created to realize the following strategic thrusts: secure sovereignty and territorial integrity, maintain internal stability, achieve the highest standard of preparedness on disasters, improve operations in support to global peace and security and promote good governance (DND 2018, 8). The NDS provides a framework that explains the connection between the national security objectives of the state. It also defines strategic thrusts of the defense establishment and clarifies the mission areas of the military. The document identifies *cyber security* as an external defense mission area for the military, focusing on threats such as "espionage, radicalization, crime, terrorism..." (DND 2018).

The NDS offers more insight on how the military should proceed with using cyber power by outlining the five tasks: defend the military network and infrastructures; collect foreign cyber threat intelligence and determine attribution; secure national security and military systems; support the national effort to secure cyberspace; and investigate cybercrimes under military jurisdiction (DND 2018, 17 and 44). While these are fundamental tasks in enhancing a state's capacity to play in cyberspace, the priorities of the defense establishment still hinge on technical aspects of cyber power, absent of any elaboration of how the military can integrate cyber operations with its traditional defensive missions.

The National Military Strategy 2019 (NMS) contains the most systematic discussion about the use of cyber power among the three documents examined in this paper. The NMS was published in 2019 with the objective of defining the ends, ways, and means by which the Armed Forces of the Philippines (AFP) will pursue and achieve its national military objectives, as it reflects the new realities and challenges confronting the military in a highly complex strategic environment (Office of the Deputy Chief of Staff for Plans, [OJ5] cited in De Castro 2024). The NMS serves as *the conceptual guide* on how the military can implement its strategic plans to ensure sustained efficiency and relevance for both current evolving contingencies and future security challenges.

Cyber power figures prominently in the NMS, most notably in the general framework of the strategy where cyber engagements are integrated within the full spectrum of military operations: ends (secure cyberspace), ways (cyber defense), and means (develop cyber capabilities) (OJ5 cited in Office of the Assistant Chief of Air Staff for Plans [A5] 2022). The NMS considers *cyber security* country in future wars, but confuses the utility of cyber capabilities with traditional military capabilities. For instance, the NMS emphasizes the development of cyber capabilities to *deter* adversaries without considering the research that indicates that traditional frameworks of deterrence may not apply to cyber operations (cf. Libicki 2009; Brantly 2018).

Another apparent concern is the technical aspects of cyber defense such as the protection of information infrastructure and recruitment of skilled IT personnel (OJ5 cited in A5 2022). While these are essential to cyber defense, there is barely any discussion on how cyber capabilities can enable military operations in other mission areas as well as contribute to the overall national security of the country.

Implications

Two crucial implications can be drawn from the military's limited awareness of cyber power. The first is that limited appreciation of cyber power can contribute to misleading beliefs about the strategic utility of cyber capabilities. A prominent example is that cyber capabilities are *revolutionary* because they can level the playing field between powerful and weak states in the international system. This belief is based on three arguments: cyber conflict is asymmetric, cyberspace is offense dominant, and deterrence is ineffective in cyberspace (Lynn III 2010). While some scholars continue to play up the revolutionary potential of cyber capabilities, all the arguments have been properly disputed by subsequent research (cf. Lindsay 2013; Gartzke 2013).

The second implication is that limited appreciation of cyber power can contribute to threat inflation. An infamous example of threat inflation is the concept of *cyberwarfare* or the use of computer networks to damage and disrupt the computer networks of adversaries. The threat is inflated because it assumes that military forces can operate against adversaries without considering the unique characteristics of cyberspace. While cyberwarfare may seem promising in the networked society, research suggests that cyber effect operations are not war because they fall short of the required thresholds of war (Valeriano and Maness 2016; Delerue 2020). Indeed, the concept of cyberwarfare has been discredited because it does not accurately represent the strategic outcomes that cyber operations can produce (Rid 2011; Borghard and Lonergan 2017).

BUREAUCRATIC POLITICS

The strategic use of cyber power is usually assigned to intelligence and military organizations (cf. Thomas 2009; Healey 2013; Cohen 2016), however there are variations in the case of weaker states with limited capacity (Ratha and Kunvath 2020; Purdon and Vera 2020). The designation of the primary government agency for securing in cyberspace mostly depends on a convergence of factors that shape a state's perception regarding cyber threats (Gomez and Villar 2018). While the dominant view is that cyber operations fall below the threshold of war, there is no consensus on the most effective way to organize for conflict in cyberspace (Lindsay 2021).

In the Philippines, the primary government organization responsible for all cyber issues is the Department of Information and Communications Technology (DICT), even if the organization was primarily designed for addressing cybercrimes and protecting critical infrastructure (DICT Act of

2015). National security issues such as state-sponsored cyber operations are within the purview of the Department of National Defense (DND). However, coordination between the DICT and the DND in terms of cyber operations remains unclear. To strengthen the coordination, the National Intelligence Coordination Agency (NICA) was crreated. It is tasked to develop a *national cyber intelligence network* that unites the cyber defense initiatives of both civilian and national security communities in the Philippines (Dy et al. 2023, 17–18). These new initiatives and organizations involve conflicting interests that may impact the development of a cyber force. This section draws on the literature on bureaucratic politics to explain how turf politics, silo politics, and budgetary politics, explains how differences between government agencies impede the creation of a cyber force.[5]

The first form of bureaucratic politics that emerges is turf politics. This explains how bureaus or departments are more motivated to carefully guard their own territory than to contribute dispassionately to reasoned analysis of how to achieve the public good. An illustrative example is the potential *turf battles* over responsibility for countering state-sponsored cyber intrusions against the Philippines. On one hand, the DICT is mandated to coordinate all initiatives relating to cybercrimes and critical infrastructure protection, but it has taken the lead in investigating state-sponsored cyber intrusions even without an explicit mandate to deal with national security threats (e.g. espionage, sabotage and subversion). On the other hand, the military's primary mission is to defend the state from national security threats but its role in national cyber operations remains ambiguous. Meanwhile, NICA has been reorganized to adapt to cyber and other emerging threats without any clear mandate to conduct cyber operations against adversaries (Office of the President 2024). Considering these circumstances, building a cyber force may enhance turf politics because government agencies such as the DICT, AFP, and NICA will prioritize their institutional self-interests and attempt to maximize their status by protecting their respective mandates, autonomy, and networks in relation to cybersecurity (Dunlevy 1991 cited in Hart and Willie 2012).

[5] Bureaucratic politics is an approach that "suggests that non-elected bureaucrats driven by divergent views and interests play a pivotal role in the policy process, and that policy choices emanate from opaque interaction and bargaining among multiple executive actors more so than from deliberation in democratically elected bodies" (Hart and Willie 2012, 370).

Silo politics is the second form of bureaucratic politics mentioned in this paper. This form points to the lack of desire or motivation to coordinate between entities within or among bureaus or departments whose collaboration is necessary to effectively address policy issues that transcend the mandates and resources of any single government organization. The literature on bureaucratic politics suggests that silos in Asia are "underpinned by legacies of colonial, military, or one-party rule; by hierarchical values; by a strong tradition of paternalistic, authoritarian, and centralized bureaucratic culture..." (Cheung 2016 cited in Scott 2020). Moreover, Asian bureaucracies are normally closed organizations that are subjected to limited organizational reforms and changes in the administrative culture over the years (Scott 2020).

An example of silo politics is the apparent lack of coordination between the NSC and the DICT during the previous government. In a Senate Committee hearing regarding the franchise of DITO Telecommunity Corporation, National Security Adviser Hermogenes Esperon, Jr. claimed that the Philippines had no national cyber operations center to defend the country against cyber intrusions (Gotinga 2020). He further stated that the AFP performed the threat assessments in the absence of the cyber capabilities at the national level (Gascon 2020). Although the National Security Advisor is the principal advisor of the government on national security matters, it overlooked the existence of the National Computer Emergency Response Term (CERT-PH) under the DICT (DICT Department Circular No. 003 2020). Indeed, there was no formal mechanism for breaking down silos in the National Cybersecurity Plan 2022, which mostly prioritizes domestic cyber threats and law enforcement operations (Cabanlong et al. 2017).

Another useful example of silo politics is the weak response of government agencies to DICT's Project SONAR.[6] DICT reported that only 55 of 388 government agencies responded to their vulnerability assessment reports, suggesting the limited desire to cooperate despite the persistent incidents of cyber intrusions against the Philippines (Chi 2024; Lalu 2024). While it is

[6] Project SONAR or Secure Online Network Assessment and Response System was implemented by the DICT starting December 2023. It involves the systematic scanning of computer networks and systems for vulnerabilities across the government with or without the permission of the agencies being scanned.

unlcear whether military and intelligence agencies were subjected to Project SONAR, the lack of responses from a considerable portion of the government ~~is a~~ cleary inclidates silo politics, impeding the policy coordination required to make use of the organizational capacities for securing cyberspace.

Implications

The discussion on bureaucratic politics raises at least two implications for the development of a cyber force. The first is that there is an opportunity for adversaries to exploit bureaucratic politics in government cyber organizations. Turf politics can be exploited since it can prevent AFP and NICA from efficiently sharing information with each other and with the DICT, particularly when cyber operations against the Philippines are conducted by powerful states. Silo politics can delay the coordination among AFP, DICT, and NICA. Since cyber operations are instantaneous and persistent, silo politics can weaken the capacity of the national government to effectively respond to state-sponsored cyber threats.

The second implication is that bureaucratic politics can make it difficult for a cyber force to perform its functions. Turf politics can potentially complicate the scope of military operations since the current *National Cybersecurity Plan 2023-2028* identifies NICA as the future “fusion center” for all cyber threats against the Philippines. However, it will not maintain any computer emergency response team. While a cyber fusion center is a promising framework to manage turf politics, the requirements and protocols for cyber operations are different compared to intelligence and military operations. For instance, the AFP is currently preparing to comply with the standards of the General Security of Military Information Agreement (GSOMIA) of the United States of America.[7] Can other government agencies be part of this agreement?

[7] GSOMIA is an agreement between the United States and an allied state that ensures the protection of defense-related information that is generated by, for the use of, or held by the government authorities, and that requires protection in the interests of national security.

STRATEGIC CULTURE

Strategic culture is a useful analytical concept in shaping the strategies and foreign policies of states (Lantis 2015; Kartchner et al. 2023). The influence of strategic culture on military strategy is well-established (Gray 1999). However, as discussed in the previous section, recent works have also confirmed the role of strategic beliefs and practices in explaining state behavior in cyberspace. Sadly, the role of strategic culture in shaping the military strategies and national security policies of the Philippines remains understudied. To date, there have been few studies that explicitly focus on the strategic culture of the Philippines during the past twenty-five years.[8] This section draws on the works of De Castro (2014) and Arugay (2022) to outline the characteristics of Philippine strategic culture and explicate how these characteristics can affect the development of a cyber force.

Philippine strategic culture can be characterized as insular or *inward-looking* based on the military's predisposition towards irregular warfare and its continued dependence on the United States for military assistance and security guarantees (De Castro 2014; Arugay 2022). These two characteristics are anchored on the colonial legacies of Spain and the United States. The AFP's orientation towards irregular warfare originates from the Spanish colonial rule where low-intensity conflict through raiding rather than decisive battles were the favored form of fighting among the pre-colonial tribes (Pobre 2000 cited in De Castro 2014). Similarly, the AFP's dependence on the United States for military assistance and security guarantees originates from Spanish and American colonial periods, where the Philippines was reliant on foreign powers to fill the gaps in the country's strategic requirements. Indeed, the United States established two military organizations, the Philippine Constabulary and the Philippine Scouts, which eventually became the foundations of the Armed Forces of the Philippines (McCoy 2001 cited in De Castro 2014).

The insularity of Philippine strategic culture remains adamantine because of entrenched political, economic, and social conditions. Drawing on the work of McCoy (2001), De Castro (2014) notes that preferences of around four hundred

[8] Studies on the strategic culture of the Philippines include Villacorta (1999), De Castro (2014), Arugay (2022), Gomez (2022) and Amador III et al. (2022)

elite families have shaped the political, economic, and social conditions. It has defined the status of the military during the past seven decades—preoccupied with internal security, lack of conventional capabilities, low defense budget, and dependence on the alliance with the United States. A prominent manifestation of an insular strategic culture is the enduring dominance of the Philippine Army in terms of leadership, resource allocation and personnel despite the Philippines being an archipelago.[9] Since the AFP is shifting its strategy from internal security to external defense, the dominant role of the Philippine Army in this new strategic direction needs to be carefully evaluated. Another indication of the insular nature of strategic culture is the prominence of insurgency and terrorism as topics of academic and policy studies. The fact that academics and analysts consider irregular warfare as more relevant than air power and sea power reflects the significance of internal security operations over external defense.[10]

Implications

The insular nature of Philippine strategic culture can affect the development of a cyber force in two ways. The first relates to the focus on internal security. The predisposition of the military towards internal security can influence the cyber force to prioritize operations that support counterinsurgency and counterterrorism missions. While militant organizations are significant threats to national security, they do not have the capacity to effectively challenge states using cyber power (Kenney 2015). States continue to be the most powerful actors in cyberspace as illustrated by cases such as Operation Orchard, Operation Olympic Games, and Operation Socialist (Lindsay 2013; Boffey 2018; Gross 2018). Within this context, using cyber operations for internal security operations is counterproductive and defeats the purpose of using cyber power strategically (Gray 2013).

[9] Forty out of the fifty-seven AFP Chiefs-of-Staff were from the Philippine Army. The Philippine Army consistently receives more funding from the government compared to the other military services. It employs more personnel than the Philippine Air Force and Philippine Navy combined (Parameswaran 2019).

[10] Studies on counterinsurgency and counterterrorism are more substantial compared to other topics related to military affairs. Selected works include Banloi (2005), Ferrer (2007), De Castro (2010), Ugarte and Turner (2011), Kalicharan (2019), Engelbrecht (2021), Smith and Bajo (2024), Ouassini and Ouassini (2024), among others.

The second way an insular strategic culture can affect the development of a cyber force is by reinforcing the dominance of the Philippine Army. The Philippine Army has been the dominant military service for the past seventy years, but no longer is this sustainable given the unique characteristics of cyberspace. While the Philippine Army may have considerable capabilities for computer network operations, this does not mean it should build and manage the cyber force of the AFP. Since each of the Philippine Army's doctrine is anchored on irregular warfare, an Army-dominated cyber force may prioritize the use of cyber power for internal security operations rather than its envisioned purpose of defending against the most consequential state-sponsored cyber operations.

CONSIDERATIONS IN BUILDING A CYBER FORCE

This section offers some recommendations that may help lessen the struggle to build a cyber force in the Philippines. The first recommendation addresses the limited appreciation of cyber power. A useful approach to improving understanding about the strategic utility of cyber power is to introduce courses that investigate the implications of established and emerging technologies on military forces. A course can be incorporated into the curriculum of professional military educational institutions in the Philippines.[11] For instance, it can be offered jointly by the Department of Social Sciences and Department of Information and Computing Sciences of the Philippine Military Academy. It can also be offered as a short course under the different education and trainings units coordinated by the Office of the Deputy Chief of Staff for Education, Training, and Doctrine (J8).

The second recommendation relates to bureaucratic politics. The ambiguity regarding which agency should lead the national effort to secure cyberspace can be managed through the National Cybersecurity Inter-Agency Committee (NCIAC) because all relevant government agencies are part of the committee. Although the recommendation to empower the NCIAC is already indicated in the National Cybersecurity Plan 2023-2028. Several issues remain unclear including the protocols to determine when a cyber incident escalates to a national security

[11] The course can be patterned after the Technology and International Security (NSA 206) module of the Master in National Security Administration (MNSA) of the National Defense College of the Philippines.

issue (e.g. state-sponsored intrusions), the measures to address the refusal of agencies to share classified information (e.g. military versus civilian agencies), and most importantly, clarifying the lead government agency that takes charge of all cyber affairs (e.g. DICT versus DND versus NICA).

The third recommendation relates to strategic culture. The first consideration to manage the insular strategic culture of the Philippines is for Congress to decrease resources allotted for internal security operations. Research suggests that military force is just one component of counterinsurgency and counterterrorism operations. It is unclear why the Philippine Army continues to employ substantial resources and personnel against the *strategically defeated* Communist Party of the Philippines – New People's Army (CCP-NPA) (Malaya cited in Rita 2024). Reallocating the resources for territorial defense is imperative if the Philippine Army intends to align with the new Comprehensive Archipelagic Strategy Concept (CADC) that prioritizes external threats against the Philippines.

A second consideration is to leverage on the Philippine-United States alliance to acquire fundamental capabilities that modern military forces utilize such as ground-based air surveillance radars, Command, Control, Communications, Computers Intelligence, Surveillance and Reconnaissance (C4ISR) battle management systems, and maritime domain awareness systems.[12] The focus on developing fundamental capabilities is consistent with the Self-Reliant Defense Posture Revitalization Act which aims to build the capacity of the military to counter external security threats through "locally produce advanced weaponry and equipment for its armed forces through technology transfer, partnerships with, and incentives to, the private sector" (Self-Reliant Defense Posture Revitalization Act 2024).

[12] C4ISR are capabilities that can provide advantage through situational awareness, knowledge of the adversary and environment, and shortening the time between sensing and response (Northrop Grumman 2024).

CONCLUSION

Cyber forces are vital assets that states utilize to protect and advance their national security interests in the twenty-first century. While a considerable number of states are preparing to deploy their cyber forces, the Philippines is still evaluating how cyber power is best employed to shape its diplomatic and military interactions. In this context, this paper evaluated the prospects of developing a cyber force from a strategic perspective. It analyzed the military's struggle to build a cyber force by exploring three internal factors that affect the military: limited appreciation of cyber power, bureaucratic politics, and the insularity of Philippine strategic culture.

The military's limited sense of cyber power is the first factor that may affect the development of a cyber force because it can contribute to misleading beliefs about the strategic utility of cyber power as well as facilitate the exaggeration of threats emanating from cyberspace. Bureaucratic politics is another factor that can complicate the development of a cyber force because it gives adversaries the opportunity to exploit the tension between government cyber organizations as well as make it difficult for a cyber force to perform its functions. An insular strategic culture is the third factor that can affect the development of a cyber force. It directs the military's focus towards international security operations which reinforces the belief and practice of the Philippine Army's dominance over other military units.

The paper offers several considerations that may address the factors that affect the development of a cyber force. The military can better appreciate cyber power if professional military education includes courses on the implications of established and emerging technologies on military forces. An effective NCIAC is instrumental in enabling the development of a cyber force. It is a strong position to manage bureaucratic politics between government agencies. Convincing the military to reallocate resources from internal security to territorial defense as well as leveraging the Philippine-United States alliance to acquire fundamental capabilities for territorial defense are concrete steps in managing the insular strategic culture of the Philippines.

GOVERNMENT DOCUMENTS

Cabanlong, Allan. S. et al. *National Cybersecurity Plan 2022*. Department of Information and Communications Technology, 2017. https://dict.gov.ph/national-cybersecurity-plan-2022

Dy, Jeffery. I. C. et al. *National Cybersecurity Plan 2023-2028*. Department of Information and Communications Technology, 2023. https://dict.gov.ph/national-cyber-security-plan

Department of National Defense. *National Defense Strategy 2018-2022*. Department of National Defense, 2018. https://www.globalsecurity.org/military/library/report/2018/philippines-national-defense-strategy_2018-2022_201811.pdf

Executive Order No. 54. "Reorganizing The National Intelligence Coordinating Agency and For Other Purposes." 24 January 2024. https://www.officialgazette.gov.ph/2024/01/19/executive-order-no-54-s-2024/

National Security Council. 2018. *National Security Strategy*. https://nsc.gov.ph/images/NSS_NSP/NSS_2018.pdf

Office of the Assistant Chief of Air Staff for Plans, Philippine Air Force. Theory of Victory In *The Future of Philippine Warfare Vol II,* edited by Ferdinand M. Cartujano. National Defense College of the Philippines, 2022. https://ndcp.edu.ph/wp-content/uploads/2022/10/FPW-Vol2.pdf

Republic Act No. 10844. "An Act Creating the Department of Information and Communications Technology, Defining Its Powers and Functions Appropriating Funds therefor, and for Other Purposes." 23 May 2016. https://issuances-library.senate.gov.ph/sites/default/files/2023-02/ra%252010844.pd

Republic Act No. 12024. "An Act Revitalizing and Strengthening The Self-Reliant Defense Posture Program And Promoting The Development of A National Defense Industry Pursuant Thereto And Providing Funds Therefor." 8 October 2024. https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/2/97883

United States Department of Defense. 2010. *Joint Terminology for Cyberspace Operations*. https://nsarchive.gwu.edu/media/21369/ocr

REFERENCES

Amador, Julio S., Deryk Matthew Baladjay, and Sheena Valenzuela. 2022. "Modernizing or Equalizing? Defence Budget and Military Modernization in the Philippines, 2010– 2020." *Defence Studies* 22 (3): 299–326. https://doi.org/10.1080/14702436.2022.2030713

Arugay, Aries A. 2022. "Defying the Water's Edge: The Philippines and Its Strategic Policy toward the United States-China Competition," in *The New Normal of Great Power Competition: The U.S.-China-Russia Relationship and the Indo-Pacific Region,* ed. The National Institute for Defense Studies. Tokyo: The National Institute for Defense Studies.

Banloi, Rommel C. 2005. "Maritime Terrorism In Southeast Asia: The Abu Sayyaf Threat" *Naval War College Review* 58 (4): 62–80. https://digital-commons.usnwc.edu/nwc-review/vol58/iss4/7

Blessings, Jason. 2019. "The Diffusion of Cyber Forces: Military Innovation and the Dynamic Implementation of Cyber Force Structure," PhD dissertation, Syracuse University. https://surface.syr.edu/etd/1190/

Boffey, Daniel. 2018. "British spies 'hacked into Belgian telecoms firm on ministers' orders." *Guardian,* 21 September. https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report

Borghard, Erica D. and Lonergan, Shawn W. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26 (3): 452–481. https://doi.org/10.1080/09636412.2017.1306396

Brantly, Aaron F. 2018. "The Cyber Deterrence Problem," in *10th International Conference on Cyber Conflict CyCon X: Maximising,* eds. Tomáš Minárik, Raik Jakschis, and Luria Lindström. Slovania: NATO CCDCOE Publications. https://ieeexplore.ieee.org/document/8405009

——— and Smeets, Max. 2020. "Military Operations in Cyberspace," in *Handbook of Military Sciences,* ed. Anders McD Sookermany. New York: Springer Publishing.

Buchanan, Ben. 2020. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Boston: Harvard University Press.

Calderaro, Andrea and Anthony J.S. Craig. 2020. "Transnational governance of cybersecurity: Policy Challenges and global inequalities in cyber capacity building." *Third World Quarterly* 41 (6): 917–38. https://doi.org/10.1080/01436597.2020.1729729

Chesney, Robert, Max Smeets, Johsua Rovner, Michael Warnerand, Jon R. Lindsay, Michael P. Fischerkeller, Richard J. Harknett, and Nina Kollar. 2020. "Policy Roundtable: Cyber Conflict as an Intelligence Contest." *Texas National Security Review* 3 (4): 2–88. http://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/

Chi, Cristin. 2024. "DICT: Most gov't agencies failed to respond to cybersecurity warnings." *Philippine Star,* April 30. https://www.philstar.com/headlines/2024/04/30/2351583/dict-most-govt-agencies-failed-respond-cybersecurity-warnings

Clark, David. D. and Susan Landau. 2011. "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks*, ed. Committee on Deterring Cyberattacks. Washington DC: National Academies Press.

Cohen, Matthew S., Charles D. Freilich, and Gabi Siboni. 2016. "Israel and Cyberspace: Unique Threat and Response." *International Studies Perspectives* 17 (3): 307–21. https://www.jstor.org/ stable/26393471

Craig, Anthony J. S. and Brandon Valeriano. 2018. "Realism and Cyber Conflict: Security in the Digital Age," in *Realism in Practice: An Appraisal*, ed. Davide Orsi, J. R. Avgustin, and Max Nurnus. Bristol: E-International Relations Publishing.

Crismundo, Kris. 2023. "Ransomware attacks in PH jump by 57.4% in 2022." *Philippine News Agency,* 22 March. https://www.pna.gov.ph/articles/1197997

De Castro, Renato C. and Walter Lohman. 2012. *Getting the Philippines Air Force Flying Again: The Role of the U.S.–Philippines Alliance*. Washington DC: The Heritage Foundation

———. 2010. "Abstract of Counterinsurgency in the Philippines and the Global War on Terror. Examining the Dynamics of the Twenty-first Century Long Wars." *European Journal of East Asian Studies* 9 (1): 135-60. https://doi.org/10.1163/156805810X517706

———. 2014. "Philippine Strategic Culture: Continuity in the Face of Changing Regional Dynamics." *Contemporary Security Policy* 35 (2): 249–69. https://doi.org/10.1080/13523260.2014.927673

———. 2024. "Exploring the Philippines' Evolving Grand Strategy in the Face of China's Maritime Expansion." *Journal of Current Southeast Asian Affairs* 43 (1): 94–119. https://doi.org/10.1177/1868103424123467

Delerue, F. 2020. *Cyber Operations and International Law*. England: Cambridge University Press.

Domingo, Francis. 2022. *Making Sense of Cyber Capabilities for Small States*. London: Routledge.

———. 2024. "Made in China? The Challenge of State-Sponsored Cyber Intrusions in the Philippines." *ISEAS Fulcrum*, 4 March. https://fulcrum.sg/made-in-china-the-challenge-of-state-sponsored-cyber-intrusions-in-the-philippines/\

Engelbrecht, Georgi. 2021. "The Logics of Insurgency In The Bangsamoro." *Small Wars & Insurgencies* 32 (6): 887–912. https://doi.org/10.1080/09592318.2021.1940424

Ferrer, Miriam C. 2007. "The Communist Insurgency," in *A Handbook of Terrorism and Insurgency in Southeast Asia,* eds. Andrew T.H. Tan. Cheltenham: Edward Elgar Publishing Ltd

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (2): 41–73. https://doi.org/10.1162/ISEC_a_00136

Gascon, Melvin. 2020. “Senators alarmed gov’t helpless to counter cyberthreats.” *Philippine Daily Inquirer.* 8 December. https://newsinfo.inquirer.net/1369152/senators-alarmed-govt-helpless-to-counter-cyberthreats

Gotinga, JC. 2020. “PH has no cybersecurity operations center, says Esperon in Dito Telecom hearing. *Rappler,* 7 December. https://www.rappler.com/philippines/esperon-says-philippines-no-cybersecurity-operations-center-senate-hearing-dito-telecom/

Gomez, Miguel A.N. 2016. Arming Cyberspace: The Militarization of a Virtual Domain. *Global Security and Intelligence Studies* 1 (2): 42–65.

——— and Villar, Eula B. 2016. “Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats.” *Politics and Governance* 6 (2): 61–71. https://www.cogitatiopress.com/politicsandgovernance/article/view/1279

———. 2021. “Overcoming Uncertainty in Cyberspace: Strategic Culture and Cognitive Schemas.” *Defense Studies* 21 (1): 25–46. DOI: 10.1080/14702436.2020.1851603

Gray, Collin S. 2013. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Carlisle: U.S. Army War College Press.

———. 1999. “Strategic Culture as Context: The First Generation of Theory Strikes Back.” *Review of International Studies* 25 (1): 49–69. https://doi.org/10.1017/S0260210599000492

Gross, Judah A. 2018. “Ending a decade of silence, Israel confirms it blew up Assad’s nuclear reactor.” *Times of Israel,* 21 March. https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/

Hart, Paul and Anchrit Willie. 2012. “Bureaucratic Politics: Opening the Black Box of Executive Government” In *The SAGE Handbook of Public Administration,* eds. B. Guy Peters and Jon Pierre. London: Sage Publications Ltd.

Hayden, Michael V. 2016. *Playing to the edge: American intelligence in the age of terror*. New York: Penguin Random House.

Healey, Jason, ed. 2013. *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*. Virginia: Cyber Conflict Studies Association.

Hutchins, Eric M., Michael J. Cloppert, Rohan M. Amin. 2011. “Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” in *Leading Issues in Information Warfare and Security Research,* ed. Julie Ryan. Singapore: Academic Publishing International Limited.

Inosate, Aubrey Rose A. 2024. PHL seen to Increase Cybersecurity Funding Due To Rising Threats. *Business World,* 12 April. https://www.bworldonline.com/corporate/2024/04/12/587598/phl-seen-to-increase-cybersecurity-funding-due-to-risingthreats/#:~:text=CYBERSECURITY%

Kartchner, Kerry M., Briana D. Bowen, and Jeannie L. Johnson. 2023. *Routledge Handbook of Strategic Culture.* London: Routledge.

Kallender, Paul and Christopher W. Hughes. 2016. “Japan’s Emerging Trajectory as a ‘Cyber Power’: From Securitization to Militarization of Cyberspace.” *Journal of Strategic Studies* 40 (1-2): 118–45. https://doi.org/10.1080/01402390.2016.1233493

Kaska, Kadri, Anna-Maria Osula, and Jan Stinissen. 2013. *The Cyber Defence Unit of the Estonian Defence League*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Kenney, Michael. 2015. “Cyber-Terrorism in a Post-Stuxnet World.” *Orbis* 59 (1): 111–28. https://doi.org/10.1016/j.orbis.2014.11.009

Kalicharan, Veera Singam. 2019. “An Evaluation of the Islamic State’s Influence over the Abu Sayyaf.” *Perspectives on Terrorism* 13 (5): 90–101. https://www.jstor.org/stable/26798580

Korolov, Maria and Lysa Myers. 2022. What is the cyber kill chain? A model for tracing cyberattacks. *CSO Online*. 14 April. https://www.csoonline.com/article/539916/what-is-the-cyber-kill-chain-a-model-for-tracing-cyberattacks.html

Kostyuk, Nadiya. 2024. Allies and Diffusion of State Military Cyber Capacity, *Journal of Peace Research* 61 (1): 1–15. https://doi.org/10.1177/0022343324122655

Lalu, Gabriel Pabico. 2024. DICT: Only 55 of 388 gov’t Agencies Responded on Online Vulnerabilities. *Philippine Star*, 30 April. https://www.philstar.com/headlines/2024/07/17/2370848/cybersecurity-team -effort-dict-says-after-hack-attack-dmw

Lantis, Jeffrey S. 2015. *Strategic Cultures and Security Policies in the Asia-Pacific*. London: Routledge.

Loo, Bernard F. W. 2020. “The Challenges Facing 21st Century Military Modernization.” *Prism* 8 (3): 137–56. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2054165/the-challenges-facing-21st-century-military-modernization/

Longhurst, Kerry. 2004. *Germany and the Use of Force*. Manchester: Manchester University Press.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Lindsay, Jon R. 2013. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22 (3): 365–404. https://doi.org/10.1080/09636412.2013.816122

———. 2021. “Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a large-scale intelligence problem.” *Intelligence and National Security* 36 (2): 260–78. https://doi.org/10.1080/02684527.2020.1840746

Lynn III, William J. 2010. "Defending a New Domain: The Pentagon’s Cyberstrategy." *Foreign Affairs* 89 (5): 97–108. https://www.jstor.org/stable/20788647

McCoy, Alfred F. 2001. “The Colonial Origins of Philippine Military Traditions,” in *The Philippine Revolution of 1896: Ordinary Lives in Extraordinary Times*, eds. F. Rodao and F. N. Rodriquez. Quezon City: Ateneo De Manila University.

McGuffin, Chris., and Paul Mitchell. 2014. “On Domains: Cyber and the Practice of Warfare.” *International Journal* 69 (3): 394–412. https://doi.org/10.1177/0020702014540618

Northrop Grumman. *nd.* “What is C4ISR?” https://www.northropgrumman.com/c4isr

Nye, Joseph S. 2011. *The Future of Power*. New York: PublicAffairs.

Ouassini, Nabil. and Anwar Ouassini. 2024. “Between Criminality and Terrorist Violence: The Abu Sayyaf Group in the Philippines,” in *Handbook of Terrorist and Insurgent Groups*: *A Global Survey of Threats, Tactics, and Characteristics,* eds. Scott N. Romaniuk, Animesh Roul, Amparo Pamela Fabe, János Besenyő. London: CRC Press.

Parameswaran, Prashanth. 2019. “What Does the New Philippines Defence Budget Say About Future Military Modernization Under Duterte? A Look at What the New Proposed Allocations Say about the Country’s Defence Outlook for 2020 and Beyond.” *The Diplomat*. 28 August. https://thediplomat.com/2019/08/what-does-the-new-philippinesdefense-budget-say-about-future-military-modernization-under-duterte/

Pernik, Piret. 2020. “National Cyber Commands,” in *Routledge Handbook of International Cybersecurity*, eds. Eneken Tikk and Mika Kerttune. London: Routledge.

Pobre, Cesar P. 2000. *History of the Armed Forces of the Filipino People*. Quezon City: New Day Publishers.

Purdon, Lucy and Francisco Vera. 2020. “Regional cybersecurity approaches in Africa and Latin America,” in *Routledge Handbook of International Cybersecurity*, eds. Eneken Tikk and Mika Kerttunen. London: Routledge.

Rattray, Greggory. 2009. “An Environmental Approach to Understanding Cyberpower,” in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Nebraska: Potomac Books, Inc.

Rid, Thomas. 2012. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35 (1): 5–32. https://doi.org/10.1080/01402390.2011.608939

Lim, Ratha and Sok Kunvath. 2020. “Sub-Regional Views on International Cybersecurity CLMV Countries,” in *Routledge Handbook of International Cybersecurity*, eds. Eneken Tikk, Mika Kerttunen. London: Routledge.

Rita, Joviland. 2024. “NSC nixes calls to abolish NTF-ELCAC.” *GMA Integrated News*, 13 May. https://www.gmanetwork.com/news/topstories/nation/906574/nsc-nixes-calls-to-abolish-ntf-elcac/story/

Rosales, Elijah Felice. 2023. “Philippines firms most exposed to cyber attacks in ASEAN.” *Philippine Star,* 21 September. https://www.philstar.com/business/2023/09/21/2297755/philippines-firms-most-exposed-cyber-attacks-asean

Sheldon, John B. 2019. “Rise of Cyber Power,” in *Strategy in a Contemporary World,* 4th edition, eds. John Baylis, James J. Wirtz, and Jeannie L. Johnson. Oxford: Oxford University Press.

Scott, Ian. 2020. “Governing by Silos,” in *Oxford Research Encyclopedia of Politics*, ed. Erin Hannah. Oxford: Oxford University Press. https://oxfordre.com/politics/view/10.1093/acrefore/ 9780190228637. 001.0001/ acrefore-9780190228637-e-1414>

Smeets, Max. 2017. "A Matter of Time: On the Transitory Nature of Cyberweapons." *Journal of Strategic* Studies 41 (1-2): 6–32. https://doi.org/10.1080/01402390.2017.1288107

———. 2022. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. Oxford: Oxford University Press.

———. 2023. “The challenges of military adaptation to the cyber domain: a case study of the Netherlands.” *Small Wars & Insurgencies* 34 (7): 1343–362, https://doi.org/10.1080/09592318.2023.2233159

Smith, Frank and Graham Ingram. “Organising Cyber Security in Australia and Beyond.” *Australian Journal of International Affairs* 71 (6): 642–60. doi:10.1080/10357718.2017.1320972.

Smith, Tom, and Ann Bajo. 2024. "The False dawns over Marawi: examining the post-Marawi counterterrorism strategy in the Philippines." *Journal of Policing, Intelligence and Counter Terrorism* 19 (3): 406–422. DOI: 10.1080/18335330.2024.2346472

Thomas, T. L. 2009. “Nation-state Cyber Strategies: Examples from Russian and China,” in *Cyberpower and National Security*, ed. ited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Nebraska: Potomac Books, Inc.

Ugarte, Eduardo and Mark Turner. 2011. "What is the ‘Abu Sayyaf’? How labels shape reality." *The Pacific Review* 24 (4): 397–420. https://doi.org/10.1080/09512748.2011.596558

Valeriano, Brandon and Maness, Ryan. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.

———. 2016. “Cyber Spillover: The Transition from Cyber Incident to Conventional Foreign Policy Dispute,” in Conflict in *Cyberspace: Theoretical, Strategic and Legal Perspectives*, eds. Karsten Friis and Jens Ringsmose. London: Routledge.

Villacorta, Wilfredo V. 1999. "Philippines: Nationalism and Regionalism," in *Strategic Cultures in the Asia-Pacific Region* edited by Ken Booth and Russell Trood. London: Macmillan Press Ltd.

THE UP CIDS DISCUSSION PAPER SERIES

The UP CIDS Discussion Paper Series features preliminary researches that may be subject to further revisions and is circulated to elicit comments and suggestions for enrichment and refinement. They contain findings on issues that are aligned with the core agenda of the research programs under the University of the Philippines Center for Integrative and Development Studies (UP CIDS).

CENTER FOR INTEGRATIVE AND DEVELOPMENT STUDIES

Established in 1985 by University of the Philippines (UP) President Edgardo J. Angara, the UP Center for Integrative and Development Studies (UP CIDS) is the policy research unit of the University that connects disciplines and scholars across the several units of the UP System. It is mandated to encourage collaborative and rigorous research addressing issues of national significance by supporting scholars and securing funding, enabling them to produce outputs and recommendations for public policy.

The UP CIDS currently has twelve research programs that are clustered under the areas of education and capacity building, development, and social, political, and cultural studies. It publishes policy briefs, monographs, webinar/conference/forum proceedings, and the Philippine Journal for Public Policy, all of which can be downloaded free from the UP CIDS website.

THE PROGRAM

The **Strategic Studies Program (SSP)** aims to promote interest and discourse on significant changes in Philippine foreign policy and develop capacity building for strategic studies in the country. It views the country's latest engagement with the great powers and multilateral cooperation with other states in the Asia-Pacific as a catalyst for further collaboration and multidisciplinary research among the intellectual communities in the region.

EDITORIAL BOARD

PROGRAM EDITORS

EDUCATION AND CAPACITY BUILDING CLUSTER

SOCIAL, POLITICAL, AND CULTURAL STUDIES CLUSTER

DEVELOPMENT CLUSTER

NEW PROGRAMS

EDITORIAL STAFF

Get your policy papers published. Download open-access articles.

The Philippine Journal of Public Policy: Interdisciplinary Development Perspectives (PJPP), the annual peer-reviewed journal of the UP Center for Integrative and Development Studies (UP CIDS), welcomes submissions in the form of full-length policy-oriented manuscripts, book reviews, essays, and commentaries. The PJPP provides a multidisciplinary forum for examining contemporary social, cultural, economic, and political issues in the Philippines and elsewh ere. Submissions are welcome year-around.

Get news and the latest publications.

Join our mailing list: bit.ly/signup_cids to get our publications delivered straight to your inbox! Also, you'll receive news of upcoming webinars and other updates.

We need your feedback.

Have our publications been useful? Tell us what you think: bit.ly/dearcids.

UNIVERSITY OF THE PHILIPPINES
CENTER FOR INTEGRATIVE AND DEVELOPMENT STUDIES
Lower Ground Floor, Ang Bahay ng Alumni, Magsaysay Avenue
University of the Philippines Diliman, Quezon City 1101

Telephone (02) 8981-8500 loc. 4266 to 4268
(02) 8426-0955

Email cids@up.edu.ph
cidspublications@up.edu.ph

Website cids.up.edu.ph