EXECUTIVE POLICY BRIEF

Cyber Operations and the Use of Force: Prospects for the Philippines

Christine Lisette M Castillo

6 December 2023
Issue Number 2023-07
EPB ISSN 2945-4689

INTRODUCTION

The United Nations (UN) Charter of 1945 is an instrument of international law which aims to promote the peaceful conduct of international relations. This Charter was created "to save succeeding generations from the scourge of war" and prevent global destruction brought by armed conflicts. In particular, Article 2(4) of the Charter states that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[1]

While cooperation and diplomatic relations are generally practiced by states, intensifying geopolitical tensions render competition, conflict, and war inevitable. This reality was reflected in the same Charter where the use of force is allowed under two circumstances: first, if it is authorized by the UN Security Council (Article 42); and second, if it is done for self-defense (Article 51).[2] In the physical domain, what qualifies as a use of force may be easily identified, such as an armed attack. In the cyber domain, however, identification can be challenging. Without an established international law on cyber operations, there would be no tool to prevent threat actors from continuing to exploit the cyber domain and conducting unlawful cyber operations. This concern, together with the alarming cyber threat landscape, necessitates further discussion.

The presence of cyber attacks is a reality for the Philippines today and will most likely remain in the immediate future. This suggests that the country needs to be better equipped and better prepared for what lies ahead. While the Philippines develops its cyber capabilities, identifying prospects drawn from a better understanding of cyber operations may aid the Philippines in dealing with cyber attacks. In support of this, this policy brief aims to tackle cyber operations and international law, and how this understanding can be beneficial for the development of cyber defense and in broad, cybersecurity.[3] In particular, this paper seeks to answer the questions:

a. What are cyber operations? How can cyber operations be determined as a use of force?
b. How do cyber operations and international law figure in the future of cyber defense and cybersecurity in the Philippines?

MAJOR CASE ISSUES

CYBER OPERATIONS AND THE USE OF FORCE IN CYBERSPACE

Cyber operations is defined by the National Institute of Standards and Technology (NIST) as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[4] To note, this definition is closely similar to what the Philippines currently uses. The types of cyber operations include intelligence collection operations, defensive cyber operations, and offensive cyber operations. For the purpose of this paper, defensive and offensive cyber operations will be highlighted. Defensive cyber operations involve passive and active operations such as internal defense measures and response to cyber attacks respectively, with the goal of defending one's network. This is more commonly employed daily in ensuring that networks are secure and well-defended.

Offensive cyber operations, meanwhile, refer to the conduct of cyber attacks. The Cyber Kill Chain framework developed by Lockheed Martin was derived from the military kill chain and is most commonly used to explain how a cyber attack takes place. It has seven steps: reconnaissance, which involves identification of target and exploration of its vulnerabilities; weaponization, or the creation of malware as an attack vector and back doors for continued access to the target system; delivery or the launching of the attack; exploitation; installation, where the attack vector will be installed in the system; command and control, where the attacker gains remote control of the target entity; and actions on objectives, which involve data theft, encryption of files, and other actions satisfying the desired goals. Monetization, the eighth step, was added over time because it has been a common motivation for cyber attacks.[5]

The Cyber Kill Chain framework provides both an advantage and a disadvantage. On the one hand, it outlines how cyber attackers operationalize an attack and is likewise used to identify solutions to thwart it by identifying at which points the attackers can be prevented, detected, or intercepted. On the other hand, the prevalence of this framework allows the attackers to be knowledgeable on how organizations strengthen their defenses and where to avoid points of detection.[6]

The use of force in and through cyberspace usually refers to offensive cyber operations. As earlier mentioned, the UN Charter allows the use of force as a countermeasure when another state employs an armed attack. When applied to cyberspace, Rule 69 of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations states that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[7] The keywords here are 'scale' and 'effects' which refer to the quantitative and qualitative aspects of cyber operations. This also means that for a cyber operation to qualify as a use of force, it must have seriously injured or killed a number of people and caused significant destruction or damage to property, as that of a kinetic use of force.[8]

Aside from scale and effects, Tallinn 2.0 particularly identifies eight (8) factors that may be considered in this task: severity; immediacy; directness; invasiveness; measurability of effects; military character; state involvement; and presumptive legality. Among these factors, severity and measurability of effects are similar to scale and effects. Severity, the most significant among the factors, refers to scope, duration, and intensity, and can be determined when a cyber operation impinges greatly on critical national interests. Meanwhile, measurability of effects is determined when consequences are apparent. In cyberspace, it is usually more challenging to quantify the consequences as compared to those in a kinetic operation. It can nevertheless be considered based on the amount of data corrupted, the number of servers compromised, and the number of data stolen, among others similar consequences. Military character and state involvement are also interesting factors to consider. Military character relates to the military nature of the traditional use of force or the military character of the target of attacks, while state involvement refers to the extent of involvement of a state to the cyber operation.[9]

One of the most well-known cyber operations is Stuxnet which targeted Iranian nuclear enrichment facilities. The Stuxnet worm was discovered in 2010 but was noted to be operational since 2005. The cyber operations temporarily derailed Iran's nuclear program; it damaged one fifth of the nuclear centrifuges, infected over 200,000 computers, and degraded 1,000 machines. Because of the impact of the operations, Stuxnet was regarded as the first cyber weapon to be developed.[10] On the one hand, classifying Stuxnet as a use of force in cyber may have merit if the scale and effects of the operations are considered. On the other hand, the argument on whether the scale and effects are comparable to those in a kinetic attack may generate debates. The worm may have spread in tens of thousands of computers around the world, but there was no reported casualty, and the physical damage was limited to the intended target.[11] If Rule 69 of Tallinn Manual 2.0 was strictly applied, Stuxnet is not a use of force in cyber.

As of writing, no country has openly declared that they have been a target of a cyber operation with the use of force. This may be viewed as a strategic decision; maintaining a gray area in this aspect allows states (especially cyber powers) to have the freedom in conducting the same offensive cyber operations that they are targets of.

In the Philippine context, attention to cyberspace has grown as the country grapples with offensive cyber operations perpetrated by state and non-state actors. Most often, it is subjected to cyber attacks which are motivated by geopolitical conflicts or national security tensions. As the country upholds the rules-based international order and is a staunch advocate of international law, it is prudent to have a better understanding of international law applicable to cyber operations.

PROSPECTS FOR THE PHILIPPINES

Cyber operations in the Philippines focus on defending military networks from cyber attacks. In June 2023, the Chief of Staff of the Armed Forces of the Philippines (AFP) stressed the importance of cyber operations in defense.[12] Although it is more feasible and practical to develop cyber defense rather than offensive capabilities, the occurrence of offensive cyber operations targeting the country cannot be denied. With limited offensive capabilities, the Philippines can first refer to international law as it is important to have a clearer understanding of how international law can apply to cyber operations.

The Philippines is a target of offensive cyber operations due to the vulnerability of networks and systems in the country as well as the geopolitical issues it is involved in. This was exemplified in 2016, when after the Philippines won the arbitral ruling on the South China Sea (SCS) dispute, at least 68 Philippine government websites suffered distributed denial of service (DDoS) attacks from China-based threat actors.[13] More recently in August 2023, Chinese advanced persistent threat (APT) group Mustang Panda compromised a Philippine government entity for at least five (5) days[14] at the height of tensions in the SCS when a Chinese coast guard vessel blocked and fired a water cannon against Philippine Coast Guard vessels escorting resupply ships bound for Ayungin Shoal.[15] The AFP has also admitted that the stolen data from its systems in 2021 are still circulating in the dark web at present, although these are regular and non-classified files.[16]

While these attacks are definitely national security issues, it can be argued that no cyber attack against the country has been classified as a use of force yet if the scale and effects are considered, including the aforementioned eight (8) factors. For instance, the usual website defacements or hacking of government websites by APT groups–although creating a huge risk for privacy and security–are not considered a use of force. These activities have political motivations and do not intend to cause harm as that generated from a kinetic attack. In addition, while the recent ransomware attack on Philippine Health Insurance Corporation (PhilHealth) by the Medusa ransomware group has exposed 13 million user data which includes all private and personal information, it still does not qualify as a use of force.[17] This incident, including all data theft in previous years, did not result in consequences similar to that of a kinetic attack. This argument may be overturned only when the effects of data theft do not stop virtually and transcend to the physical domain which result in huge loss of lives because of stolen medical records or private information. A use of force may also be raised when a cyber attack was employed to physically blow up the servers or data center of an entity, resulting in great physical destruction, such as the case in Stuxnet.

Nevertheless, the fact that no cyber attack against the Philippines has been a use of force yet does not suggest that government and non-government institutions should be dismissive and casual about these incidents, most especially that the ways of cyber threat actors are adaptive and innovative just as cybersecurity measures to counter them are. This must also be considered together with the exponential use of emerging technologies such as artificial intelligence (AI). The opportunities and risks associated with the development and use of AI is a reality. The Philippines must deliberately consider how these technologies apply according to the country's current situation and future interests.

In prospect, the country will continue to be subjected to cyber attacks. Addressing these will require the continuous development of cyber defense and enhancement of cybersecurity initiatives, including harnessing the potential of emerging technologies. A better understanding of international law applicable to cyber operations is crucial for the Philippines to be equipped enough to anticipate and prepare for all the changes and challenges ahead.

POLICY CONSIDERATIONS

Cyberspace is complex, uncertain, and highly-dynamic. New trends and developments always occur, which states have to keep up with in order to achieve cybersecurity. In connection with this, it is also important to discuss cyber operations amid the security issues facing the Philippines in national, regional, and global affairs. Having a better understanding of cyber operations in the context of the country contributes to the development of cyber defense. The following policy considerations may aid the Philippines, especially the defense establishment, in this pursuit.

Employ foresight through exploring the integration of artificial intelligence (AI) in cyber defense

It has been noted that technologies such as AI are important in military operations, particularly in predicting battlefield outcomes.[18] AI can also be used to sift through piles of classified and unclassified data and provide a prediction of future international events, including the behavior and thoughts of adversaries.[19] This has certain advantages for the military not only during war and conflicts but also during peacetime. Two forms of AI that may be explored are generative and predictive AI. Generative AI identifies patterns to generate or create new content based from the user's specified request.[20] An example is ChatGPT which caught the world's attention because of the opportunities and challenges associated with its use and development.[21] Meanwhile, predictive AI analyzes large amounts of current and historical data to forecast future events.[22] This may be utilized in geopolitical scenarios where one state would want to know the adversary's future plans based from the latter's policies, actions, and interests.[23]

In connection with this, the dual effects of AI must also be considered. This was stressed by Dr Geoffrey Hinton, the ‘godfather of AI,’ when he quit Google to freely express his thoughts on the dangers of AI, an innovation he helped develop. Dr Hinton noted the fear associated with AI chatbots for instance, which hold intelligence much higher than any human.[24] For a country which promotes digital transformation and navigates its complexities, the Philippines will benefit from the establishment of ethics, safeguards, and regulations on the use of emerging technologies in general and in armed conflicts.

It can be argued that AI will provide advantages for cyber defense in the country. However, it is equally important to employ foresight in exploring the how best to move forward with AI regarding safety and security.

Consider the inclusion of innovation power in defense and security policy documents

Several studies have noted that technology will heavily figure in the future of geopolitics and global power. In his Foreign Affairs article “Innovation Power: Why Technology Will Define the Future of Geopolitics,” Eric Shmidt argued that Ukraine’s success in the ongoing war with Russia can be credited to the former’s ‘innovation power’ or the “ability to invent, adopt, and adapt new technologies.” Technology is the one critical aspect where Ukraine proved nimbler against Russia, given that the latter has supremacy in traditional military power. This further suggests that innovation power aids military power and will continue to do so for future wars.[25] More discussions on this concept may help the Philippines deal with cyber operations at present and beyond.

In the Philippines, the inclusion of innovation power in the following key documents would provide more context on the future of cyber defense in the country and plans to build its capabilities: a) Strategic Assessment Report (SAR) of the Department of National Defense (DND); b) the National Security Strategy (NSS) of the National Security Council (NSC), as related to the national security interest of Cyber, Information, and Cognitive Security in the National Security Policy (NSP) 2023-2028; and c) policy documents on cyber operations of the AFP.

A critical factor that will help the Philippines in building its innovation power is collaborating with the United States and other security partners on AI and its application in the Philippines. It was noted that AI helped the US predict Russia’s invasion of Ukraine, eliminating the element of surprise and to an extent, limiting the effects of Russia’s cyber operations.[26] The US sent a hunt forward team of the US Cyber Command to Ukraine in late 2021 to look into Russia’s malicious cyber activity and assist Ukraine in strengthening its cyber defense.[27]

In this manner, the consistent development of AI with the help of the US will allow the Philippines to respond to national security challenges such as its claim to the West Philippine Sea. By looking into China’s actions in the South China Sea and the Chinese government’s policy pronouncements over the years, information may be generated on the country’s next courses of action, thereby providing opportunity for the Philippines to prepare for possible aggressions, increased presence, and international law violations.

Expand the recruitment of cyber warriors beyond the military by collaborating with private cybersecurity companies

In recent months, the AFP leadership has announced that it has plans to create a Cyber Command, one which has more resources, personnel, and authority in responding to cyber attacks and enhancing the country's cyber defense. Part of this plan is to recruit cyber warriors who are soldiers with technical expertise and skills on cybersecurity, and whose physical skills as those of the military are not necessary. Collaborating with private cybersecurity companies in this regard is beneficial for the armed forces because of the former's capability to share knowledge and experience in addressing cyber attacks. In addition, they can also help in providing training services for military officers who are interested in joining the Cyber Command. This will enable the Cyber Command to build its capabilities fast, which is crucial given that the military network is being targeted almost daily by local and foreign threat actors.[28]

Consider the OODA loop model in decision-making for cyber operations

The OODA loop–which stands for Observe, Orient, Decide, and Act–is a tool developed by US military strategist and Air Force pilot John Boyd. To observe is to gather all information related to the cyber operations. Next, it is necessary to do an orientation of what has been found in the observation phase, assessing whether the cyber operations have high or low impact, and identifying possible scenarios for certain decisions. Next is making a decision in consideration of all potential outcomes. Finally, actions are necessary to operationalize the decision and any changes related to this. (See Figure 1. OODA Loop Model on page 8)

Boyd believed that the key to success is quick decision-making and the ability to rapidly change actions given an uncertain and also changing environment. This logic is applicable to cyberspace given that the domain is dynamic and uncertain by nature. Without the ability to quickly assess the cyber attack, the threat actor's chance of success grows higher and the chance of success for countermeasures or reducing the damage will diminish.[29] In cyberspace, where the ability to decide and act quickly is necessary, the OODA loop will help the defense establishment hinder the success of cyber attacks and minimize disruptive consequences. As the OODA loop model is traditionally used for military operations, further research is necessary for its feasibility in the case of the Philippines.

CONCLUSION

A productive and progressive international relations is key to maintaining international peace and security. It involves political, military, economic, cultural, diplomatic, and other means of interactions between and among states. Despite this, the current geopolitical tensions and security conflicts among states around the world suggest that armed conflict and war are inevitable. In the physical domain, international laws such as the UN Charter, International Humanitarian Law (IHL), among others, govern the conduct of military operations during armed conflict and war. However, in cyberspace, an international law on cyber operations is yet to be created and uncertainties still remain. This policy brief discussed the international law applicable to cyber operations as stated in the Tallinn Manual and explored its relevance in the Philippine context. As the country navigates both the physical and cyber domains, prospects were drawn on how the defense establishment may move forward in the fulfillment of its mandate for the country and for the people.

ENDNOTES

[1] United Nations Charter, https://www.un.org/en/about-us/un-charter/full-text. Hereafter referred to as UN Charter.
[2] UN Charter.
[3] The idea for this Executive Policy Brief was drawn from the Cyber Law and Emerging Technologies Workshop by the Indo-Pacific Centre for Military Law of the Australian Defence Force, which the author attended in November 2023.
[4] National Institute of Standards and Technology, "cyberspace operations," https://csrc.nist.gov/glossary/term/cyberspace_operations.
[5] Bart Lenaerts-Bergmans, "Cyber Kill Chain," *Crowd Strike,* October 14, 2022, https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/.
[6] Lenaerts-Bergmans, "Cyber Kill Chain."
[7] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (New York: Cambridge University Press, 2017) 330, https://doi.org/10.1017/9781316822524.
[8] Tallinn Manual 2.0, 333.
[9] Tallinn Manual 2.0, 334-336.
[10] Kaspersky, "Stuxnet explained: What it is, who created it and how it works," https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet.
[11] John Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield," *Journal of Computer & Information Law* 29*,* no. 1 (Fall 2011): 2-3, https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1697&context=jitpl.
[12] Priam Nepomuceno, "AFP exec cites importance of cyber ops to PH security," *Philippine News Agency,* June 27, 2023, https://www.pna.gov.ph/articles/1204363.
[13] Anii Piiparipen, "China's Secret Weapon in the South China Sea: Cyber Attacks," *The Diplomat,* July 22, 2016, https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/.
[14] Unit 42, "Stately Taurus Targets the Philippines as Tensions Flare in the South Pacific," *Unit 42 by Palo Alto Networks,* November 17, 2023, https://unit42.paloaltonetworks.com/stately-taurus-targets-philippines-government-cyberespionage/.
[15] Jake Kwon and Heather Chen, "Philippines accuses China of firing water cannons at its ships in the South China Sea," *CNN,* August 7, 2023, https://edition.cnn.com/2023/08/06/asia/philippines-chinese-vessels-south-china-sea-intl-hnk/index.html.

[16] CNN Philippines Staff, "AFP chief eyes setting up 'cyber command' manned by 'cyber warriors'," *CNN Philippines,* October 19, 2023, https://www.cnnphilippines.com/news/2023/10/19/afp-chief-romeo-brawner-cyber-command.html.
[17] Sundy Locus, "Data of 13 million persons compromised in PhilHealth ransomware attack," *GMA News,* October 18, 2023, https://www.gmanetwork.com/news/topstories/nation/885587/data-of-13-million-persons-compromised-in-philhealth-ransomware-attack/story/.
[18] Ravi Agrawal, "The Scramble for AI: Editor's Note," *Foreign Policy,* June 19, 2023, https://foreignpolicy.com/2023/06/19/the-scramble-for-ai/.
[19] Michele A. Flournoy, "AI Is Already at War: How Artificial Intelligence Will Transform the Military," *Foreign Affairs,* October 24, 2023, https://www.foreignaffairs.com/united-states/ai-already-war-flournoy?check_logged_in=1&utm_medium=promo_email&utm_source=lo_flows&utm_campaign=registered_user_welcome&utm_term=email_1&utm_content=20231204.
[20] The Upwork Team, "Generative AI vs. Predictive AI: Differences and Application," *Upwork,* October 3, 2023, https://www.upwork.com/resources/generative-ai-vs-predictive-ai#:~:text=Generative%20AI%20is%20designed%20to,about%20future%20events%20or%20trends.
[21] Michelle Nichols, "UN chief backs idea of global AI watchdog like nuclear agency," *Reuters,* June 13, 2023, https://www.reuters.com/technology/un-chief-backs-idea-global-ai-watchdog-like-nuclear-agency-2023-06-12/.
[22] The Upwork Team, "Generative AI vs. Predictive AI."
[23] Flournoy, "AI Is Already At War."
[24] Josh Taylor and Alex Hern, "'Godfather of AI' Geoffrey Hinton quits Google and warns over dangers of misinformation," *The Guardian,* May 2, 2023, https://www.theguardian.com/technology/2023/may/02/geoffrey-hinton-godfather-of-ai-quits-google-warns-dangers-of-machine-learning.
[25] Eric Shcmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," *Foreign Affairs,* February 28, 2023, https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics.
[26] Flournoy, "AI Is Already At War."
[27] Major Sharon Rollins, "Defensive Cyber Warfare Lessons from Inside Ukraine," US Naval Institute, June 2023, https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine.
[28] CNN Philippines Staff, "AFP chief eyes setting up 'cyber command' manned by 'cyber warriors'," https://www.cnnphilippines.com/news/2023/10/19/afp-chief-romeo-brawner-cyber-command.html; Jason Gutierrez, "Philippine military to recruit 'cyber warriors' amid growing digital threats," *Benar News,* October 19, 2023, https://www.benarnews.org/english/news/philippine/philippines-recruits-cyber-warriors-online-attacks-10192023063826.html.
[29] Taylor Pearson, "The Ultimate Guide to the OODA Loop," https://taylorpearson.me/ooda-loop/; Sarah Lewis, "OODA Loop," https://www.techtarget.com/searchcio/definition/OODA-loop.

Key Provisions

UN Charter Article 2(4)

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

UN Charter Article 42

"Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."

UN Charter Article 51

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

Tallinn Manual 2.0 Rule 69

"Definition of use of force. A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."

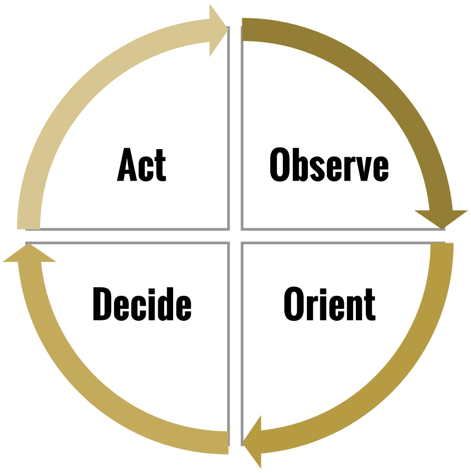

Figure 1. OODA Loop Model

NDCP Executive Policy Brief

The Executive Policy Brief (EPB) is a publication series on national defense and security issues by the Research and Special Studies Division (RSSD) of the National Defense College of the Philippines (NDCP). The views expressed in this policy brief are those of the author alone and do not necessarily reflect the views of the NDCP. The readers are free to reproduce copies mechanically, or to quote any part provided proper citations are made.

Author

Christine Lisette M Castillo is a Defense Research Officer II in the Research and Special Studies Division of NDCP. Ms Castillo's research interests include cybersecurity, cyber defense, regional and international security cooperation, and women, peace, and security (WPS). For comments on the policy brief and other related engagements, please email christine.castillo@ndcp.edu.ph.

NDCP Editorial Board

Please scan the QR code to access our Feedback Form for your comments, opinions, and suggestions. Thank you very much and we look forward to hear from you.

www.ndcp.edu.ph