NDCP Executive Policy Brief

A PUBLICATION SERIES ON NATIONAL SECURITY ISSUES
BY THE NATIONAL DEFENSE COLLEGE OF THE PHILIPPINES

28 June 2020
No. 2021 - 04

# Hybrid Warfare and Its Key Challenges: Implications in the Changing Nature of Security Environment in the Philippines

Johanna S Adap

## Introduction

Recent analyses on the geopolitical and geostrategic environment rearticulate both the philosophy and art of war[1]. This was brought by globalization, the proliferation of advanced technology, violent transnational extremists, and resurgent powers[2] resulting in complexities as it alters the nature of the security environment[3]. This is a salient issue[4] as it shows the transformation of war and new forms of belligerence emerging in the 21st century which made a number of analysts say that the nature of future combat will be blended and blurred[5]. Experts and scholars acknowledged that future adversaries will employ various techniques and procedures, both conventional and unconventional, in order to disrupt and disable the opponent's actions without engaging in open hostilities. This kind of approach features fluid and flexible combatant using advanced weapons systems for disruptive purposes, regular tactics, cyber-attacks, mass communication for propaganda, and hard-soft power to achieve victory[6]. This construct is frequently described as hybrid warfare[7]. While this is not a new trend[8], it is somehow evolving[9] as technology transforms much of the conceptualization and operationalization of war and armed conflict[10] which brings threats that are more lethal and deceptive than those of the past[11].

For the Philippines, a nation faced with different security threats, - both external and internal; and traditional and non-traditional - it is essential for the country's defense establishment to define and contextualize the future of warfare according to the peculiarities of the Philippine strategic environment, operational space, and battle experience. With the growing complexity of warfare in the 21st century, it is clear that the future wars will be fought in a hybrid manner[12].

Thus, it is important to address the current and emerging threats of hybrid warfare emanating from a variety of state and non-state actors and its implications on the Philippine defense and security. We must think broadly about security and defense challenges as many of these lie outside the traditional military domain and we are lacking of readily available ideas on how to respond to them. In particular, this paper seeks to answer the following questions: 1) What is hybrid warfare?; 2) What are the threats and challenges it poses and its implications on the Philippine strategic environment?; and 3) How can the Department of National Defense and Armed Forces of the Philippines counter the threats and challenges of hybrid warfare in the 21st century?

## Defining Hybrid Warfare

The term hybrid warfare attempts to capture the complexity of 21st-century warfare[13]. It involves both state and a variety of non-state actors[14] and blurs the traditional distinctions between types of armed conflict, and even between war and peace[15]. There are many definitions of hybrid warfare and these definitions continue to evolve to suit the changing character of contemporary war. In 2007, when Frank Hoffman defined hybrid warfare as "different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both sides and a variety of nonstate actors"[16]. Furthermore, it focuses on "multi-modal activities which are operationally and tactically directed and coordinated with the main battlespace to achieve synergistic effects"[17]. The 2014 Russo-Ukrainian War and the Chinese aggression in the South China Sea (SCS) sparked a rethinking of traditional geopolitical norms and warfare tactics.

Russia's actions in Ukraine created the current preoccupation with hybrid warfare. Western commentators used hybrid as the most appropriate term to describe the variety of methods employed by Russia during its annexation of Crimea and support to rebel militant groups in eastern Ukraine. Russian techniques included the traditional combination of conventional and irregular combat operations, and the sponsorship of political protests, economic coercion, cyber operations and, in particular, an intense disinformation campaign. The use of weaponized information is the most distinguishing feature of Russia's campaign in 2014 which combines psychological and cyber operations that seeks to blur the lines between truth and falsehood and create an alternative reality. It exploits existing societal vulnerabilities in target states, attempts to weaken state institutions and undermine the perceived legitimacy of governments[18].

**It should be noted that hybrid warfare is a challenge that is likely to persist as it is a challenge presented by the increasing complexity of armed conflict, where adversaries may combine types of warfare plus nonmilitary means to neutralize conventional military power.**

Russia is not the only state to exploit hybrid forms of warfare. It can also be seen in China's "Three Warfare" policy which shows the elements of hybrid warfare regarding its territorial claims in the South China Sea (SCS). China's action shows that it has avoided the overt use of military force, but has exploited psychological operations, media manipulation, and legal claims to advance its objectives[19]. Such approaches aim not to meet the strength of their enemies directly but to conduct coercive actions without providing clear measures that would trigger more forceful responses from the international community[20].

The Russo-Ukrainian War and the Chinese aggression in the West Philippines Sea sparked a rethinking of traditional geopolitical norms and warfare tactics. Scholars and experts determined that the methods used by these countries in times of conflict shows hybridization in character. This approach mirrors the blending and blurring character of future conflicts as it uses multimodal approach[21] which incorporates a range of different modes of warfare[22]. In other words, this approach can be employed on multiple levels at the same time which in turn, compresses the traditional levels of war – tactics, operations, and strategy – thereby accelerating the tempo at the strategic and tactical levels faster than a more conventional actor is able to do[23]. It brings threats that are simultaneous, fused, and subordinated to one command unit[24]. In such conflicts, future adversaries' means[25] to seek victory is by using a fusion of irregular tactics and the most lethal means available in order to attack and attain their political objectives[26]. It is clear that the contemporary war is multi-modal or multi-variant rather than a simple black or white characterization of one form of warfare. Indeed, hybrid wars will retain as the basic and brutal form of violence, trying to instill terror and human costs, while exploiting virtual dimensions of warfare[27]. Hence, many analysts are calling for greater attention to a more blurring and blending of war forms with increasing frequency and lethality.

On the other hand, one of the problems of discussing hybrid warfare is the lack of conceptual clarity. It has been attacked for being a catch-all phrase with limited analytical value that does not contain anything distinctly new. It is also criticized for distorting the traditional distinctions between peace, conflict and war, and for being stretched so broad as to become conceptually synonymous with grand strategy itself[28]. While these criticisms remain valid, it is also clear that the literature on hybrid warfare, as well as critics, provide fertile grounds for discussing the future of warfare as well as broader security and defense challenges[29]. Discussing hybrid warfare is meant as a common starting point for further discussion on the future security environment on how to deter, mitigate, and counter hybrid warfare threats, form states or non-state actors[30].

It should be noted that hybrid warfare is a challenge that is likely to persist as it is a challenge presented by the increasing complexity of armed conflict, where adversaries may combine types of warfare plus nonmilitary means to neutralize conventional military power[31]. Recognizing and responding effectively to hybrid warfare will become increasingly important[32]. The attempt to understand and articulate the ever-changing character of warfare is of great importance because if understood correctly, it will allow the development of a future force able to deter and defeat potential adversaries who seek new ways to win[33].

### Major Case Issues

With the peculiarities of the Philippine strategic environment, this paper discussed the current and emerging threats that will ultimately shape the security environment of the country.

### The Gray Zone Operations of China

China has been changing the geopolitical landscape of the SCS through its “gray zone” strategy – a gradualist, revisionist, and unconventional approach in altering the regional and international order in accordance with Chinese national interests[34] without the risk of open conflict[35].

The SCS is where China completely achieved the goal of hybrid warfare**.** China’s gray zone designs in the SCS give primacy to indirect methods and non-kinetic means. The construction of military-grade bases in three artificial islands (Subi, Fiery Cross, and Mischief Reefs**)**; posting of troops with missile defense capability in four others (Cuarteron, Gaven, Hughes, and Johnson South Reefs**)**; use of paramilitary fishing units in the South China Sea; conduct of regular naval and coast guard patrols[36] are effectively utilized to intimidate Filipino troops and fishermen through its “cabbage strategy” in Scarborough Shoal; and its “swarming tactics” in Philippine-controlled features in the Spratlys Islands, are clear indications that China’s maritime campaign has fully developed a new form of warfare to achieve its political objectives[37].

What is disturbing, however, is the emerging gray zone phenomenon following the “Game of Go” strategy in mainland Philippines. Using its strong economic and political influence coupled with its adeptness in covert intelligence operations, China’s strategic footprints can be gleaned from the increasing number of Chinese business interests near key Philippine maritime chokepoints and military bases as well as in critical sectors and industries, like the national power grid, telecommunications, tourism, offshore gaming operations, and transportation among others[38].

China is increasingly turning to maritime coercion through unconventional means. The concept of gray zone between war and peace is now a challenge that must take seriously and adopt strategies to counteract[39].

### Cyber Warfare

With the advent of new technology, the main hub of activity lies in the accumulation of information. Having a robust social media savvy population with few data protection mechanisms makes the Philippines extremely vulnerable to cyber-attacks and incidents[40]. Despite the government’s initiatives in 2016 in establishing the Department of Information and Communication Technologies (DICT) in conjunction with the draft National Cybersecurity Plan 2022 (NCP 2022) to meet the complex demands of this emergent and increasingly crucial domain, the question of whether the country will prove successful in its emergent role remains open to debate[41]. Indeed, we have made progress in enhancing our capability to combat cybercrime but woefully unprepared to deal with cyberterrorism and cyberwar[42].

Experts say that our vulnerability to cyber-attacks will increase exponentially with the rapid adoption of Internet of Things (IoT) as both users and manufacturers lack security awareness. From recent years, there was an increase in IoT attacks which caused damage and chaos to our power grid being put out of commission, traffic lights being out of sync, or even seismic sensors on Taal volcano shutdown or fed false information[43].

In 2016, within hours of the Permanent Court of Arbitration’s unanimous rebuke of China’s territorial claims in the South China Sea, at least 68 national and local government websites in the Philippines were knocked offline in a massive distributed denial of service (DDoS) attacks. The attacks ensued over several days, targeted key government agencies along with smaller local government units thus, limiting their ability to conduct daily functions. While China denied they were behind the attack, the context and timing are certainly critical[44].

DDoS is just the warning shot. But there are other more destructive tools designed to shut down critical national infrastructures (such as energy, transportation, government operations) and to steal or wipe out massive amounts of data that will cripple the economy[45].

This only shows that we are still at the infancy stage in our cyber security, thus, it must be a top-level concern to muster the necessary funding and to take a whole-of-nation approach[46].

### Insurgency and Terrorism

The communist insurgency and violent extremism in the Philippines has been ongoing since 1969 and shows no sign of abating[47].This is highly evident with the recent Zamboanga and Marawi siege in 2013 and 2017 respectively, and recent reports of bombing incidents especially in Mindanao. At present, the Islamic-state terrorist are believed to be taking advantage of the pandemic in recruiting and spreading violent extremism ideology in the country especially in rural areas affected by the lockdown[48]. These non-state actors use asymmetric threats to continue pursuing their strategic objectives. An essential aspect of hybridity is their capability to operate in a spectrum of violence and exploit cyberspace in a highly sophisticated manner to establish a "virtual caliphate" [49] wherein online propaganda and messaging apparatus of terrorist uses social media and encrypted communication platforms for their recruitment process. The virtual online realm is enabled to provide lessons to the participants on the narrative of global jihad[50]. These non-state actors exploited the vulnerabilities in social media to disseminate misinformation and disinformation to manipulate people to create mass chaos and insecurity, undermine trust in the government, reinforce extremist narratives, and recruitment strategies.

Furthermore, another heralded weapons of terrorist, violent extremist, and organized groups is their hacking techniques to gain unauthorized access to a system. This tactic is not designed to kill people or break physical object, rather to exclusively destroy or modify computer data to disrupt economic institutions, government websites, and power infrastructures among others, which can cause disarray on the government's daily operation and activities of the people.

It is clear that these non-state actors understand the importance of high technology to achieve their objectives. Their weapons are unique as it exist nearly exclusively in cyberspace and these can be more powerful than conventional weapons.

### Implications

Given the immense hybrid threats[51], today's security environment presents a complicating factor for defense planning in the 21st century[52]. The principal approach of future opponents will be to avoid predictability and seek advantage in unexpected ways and ruthless modes of attack. Future enemies will seek their own degree of "shock and awe" with brutality rather than precision weaponry. Indeed, irregular warfare will become normal, but with greater velocity and lethality than ever before[53].

**The implications of hybrid warfare clearly present challenges in crafting policies and strategies on dealing with its threats as well as its ambiguous forms of tactics.**

The implications of hybrid warfare clearly present challenges in crafting policies and strategies on dealing with its threats as well as its ambiguous forms of tactics. Experts suggest that in order to counter such, it is important to first detect the emerging and future hybrid threats that can damage the national interest. Identifying hybrid threats requires analysts to "connect the dots" across unfamiliar domains[54]. Thus, it may require enhanced training and more familiarity, contact, and closer working with colleagues from across the government, other nations, and multinational institutions[55].

A number of literature states that one of the effective ways to counter hybrid warfare is through deterring hybrid aggressor which can only be done if analysts were able to detect hybrid threats. However, the 1987 Philippine Constitution's renouncement of war, effectively constrains defense thinking to a reactive posture that concedes initiative to the adversary and limits the deterrence value of the Armed forces of the Philippines (AFP)[56]. Hence, the AFP should consider adopting a second-strike capability of its own to ensure that it can punish prospective aggressors, even if only as a demonstration of political resolve and defiance, to complicate the aggressor's calculation[57]. It is important to note that as capability development indicates the true implication of countering hybrid threat. Therefore, defense and security forces need to develop the ways and means required to counter such.

Success in hybrid wars also requires forces that are capable of fighting against hybrid threats. This will require appropriate training and education in order for the armed forces to recognize and quickly adapt to unknown threats. Defeating the hybrid adversary will require alterations in military and national security organizations think about strategy and in ways decision makers are informed and trained to face such challenges. It will require a leadership that can work across organizational boundaries. In addition, it will also require changes in the way military organizations acquire and exploit intelligence, and how they leverage as future adversaries are improving their ability to transfer lessons learned and techniques from one theater to another through modern information technology[58].

## Policy Considerations

This paper puts forward policy considerations as a common starting point for further discussion on the future security environment.

**Enhancement of Defense Documents.** Given the rapidly changing security environment and the complexities of the nature of warfare, it is necessary to review and update the key defense documents such as the Defense System of Management, Defense Strategic Planning System, as well as other AFP and DND crucial documents that guide our defense operations and activate our response capabilities[59]. Our defense establishment should start addressing the way adversaries will most likely engage in conflict, thus, it is of great importance to recognize and broaden the definition of hybrid warfare and its threats in these documents to make the AFP more responsive to the emerging threats and realities in our security environment.

**Build Alliances and Cooperation.** Another measure that could prove useful is to build alliances and cooperation with other states and international organizations. Working together will provide the armed forces capability development knowledge to respond efficiently and effectively. Joint research and discussions on hybrid warfare should also be conducted to better understand the nature of security threats and its vulnerabilities.

**Education and Training.** Defense and security sector must be prepared to this kind of security environment. With a proper mix of advance education and training, it will develop their cognitive skills and capabilities to make them prepared in countering both state and non-state adversaries employing unpredicted tactics.

**Upgrading of Military Materiels and Equipment.**
Along with other recommendations, there is a need to improve and modernize the equipment, materials, and facilities of the AFP to complement strategies needed for countering the threats of hybrid warfare. This would allow for greater resources to be allocated to areas that reflect the nature of 21st century warfare, such as ballistic missile defense, cyber defense, intelligence, strategic communications strategies, and tools that would address the contemporary threats and challenges.

## Conclusion

The emerging character of conflict is more complicated. Tomorrow's enemies will remain as cunning and elusive as today's foes and they may be more lethal and more implacable. Critically, the threats discussed represents a gap in the ability of defense forces to respond to contemporary challenges that are likely to endure and intensify[60]. Thus, this paper recommends some policy considerations for the DND and AFP to develop capabilities in addressing the threats of hybrid warfare. Even though the Philippines is a developing country, its perception of warfare must also evolve in step with the security environment, and ideally it must take several steps ahead of its adversaries[61]. Thus, we must think broadly about security and defense challenges and plan accordingly on the future security environment.

# # #

***Johanna S Adap** is a Training Specialist in the Research and Special Studies Division 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 NDCP. The readers are free to reproduce copies or quote any part provided proper citations are made. For comments and suggestions, please email johannaadap9@gmail.com*

**Endnotes**

[1] Yuriy Danyk, Tamara Maliarchuk and Chad Briggs. Hybrid War: High tech, Information, and Cyber Conflicts. (Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, 2017). Accessed 26 January 2021, https://www.jstor.org/stable/10.2307/26326478

[2] Frank Hoffman. Hybrid Warfare and Challenges. (National Defense Unviersity Press, 2009). Accessed 8 February 2021, https://smallwarsjournal.com/documents/jfqhoffman.pdf

[3] Ibid, 4;

[4] Laura-Maria Herta. Hybrid Warfare – A form of Asymmetric Conflict.(International Conference Knowledge-Based Organization, 2017). Accessed 15 June 2021, https://sciendo.com/downloadpdf/journals/kbo/23/1/article-p135.xml

[5] Hoffman, op. cit., 6

[6] President's Papers: The Future of Philippine Warfare Volume I, op.cit

[7] Hoffman, op. cit., 2

[8] Herta, op. cit.,1

[9] Jim Garamone. Military Must Be Ready to Confront Hybrid Threats, Intel Official Says. (US Department of Defense, 2019). Accessed 26 May 2021 from https://www.defense.gov/Explore/News/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/

[10] President's Papers: The Future of Philippine Warfare Volume I. (National Defense College of the Philippines, 2021): 78

[11] Ibid., 3.

[12] Ibid., 78.
[13]James K Wither. Defining Hybrid Warfare. Accessed 26 May 2021 from https://www.marshallcenter.org/en/publications/concordiam/perspectives-hybrid-warfare/defining-hybrid-warfare
[14] Frank G Hoffman. Conflict in the 21st century: The Rise of Hybrid Wars. (Potomac Institute for Policy Studies, 2017). Accessed 24 May 2021 from https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
[15] Wither, op. cit, 1;
[16] Ibid., 1;
[17] Laura-Maria Herta, op. cit., 22
[18] Ibid., 2;
[19] Ibid., 3.
[20] President's Papers: The Future of Philippine Warfare Volume I. op. cit.,79
[21] Frank G Hoffman. Small Wars Revisited: The United States and Nontraditional War. (Journal of Strategic Studies, Vol 28, no 6., December 2005)
[22] Frank G Hoffman. Conflict in the 21st century: The Rise of Hybrid Wars. (Potomac Institute for Policy Studies, 2017). Accessed 24 May 2021 from https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
[23] Erik Reichborn-Kjemmerud & Patrick Cullen. What is Hybrid Warfare? (Norwegian Institute of International Affairs, Policy Brief, 2016). Accessed 20 May 2021 from https://core.ac.uk/download/pdf/52131503.pdf
[24] Herta, op. cit., 2.
[25] Hoffman, op. cit., 7
[26] Ibid., 9.
[27] Frank Hoffman. Hybrid Warfare and Challenges, op. cit., 9.
[28] Erik Reichborn-Kjemmerud & Patrick Cullen, op. cit., 11.
[29] Sean Monaghan. Countering Hybrid Warfare: So What for the Future Joint Forces? (National Defense University Press, Prism, Vol 8 no 2, October 2019). Accessed 28 Feb 2021 from https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf
[30] Ayodele A Otaiku. A Framework for Hybrid Wars: Threats, Challenges, and Solutions. (Journal of Defense Management, 2018) Accessed on 23 February 2021 from https://www.longdom.org/open-access/a-framework-for-hybrid-warfare-threats-challenges-and-solutions-2167-0374-1000178.pdf
[31] Ibid., 33
[32] Ibid., 41
[33] Ibid., 57
[34] Rommel R Cordova. Philippine Strategic Approaches to Address China's Gray Zone Strategy in the South China Sea. (Asia Pacific Pathways to Progress Foundation, Inc., 22 January 2020) Accessed 27 May 2021 from https://appfi.ph/resources/commentaries/2932-philippine-strategic-approaches-to-address-china-s-gray-zone-strategy-in-the-south-china-sea
35Huseyin Korkmaz. Hybrid warfare and maritime militia in China, Accessed 13 June 2021 from https://www.aa.com.tr/en/analysis/analysis-hybrid-warfare-and-maritime-militia-in-china/1897259
[36] Op. cit., 3
[37] Emilio Marayag. China's Maritie Cmapaign in the South China Sea. (The Maritime Review, September 2019). Accessed 19 April 2021 from https://maritimereview.ph/chinas-maritime-campaign-in-the-south-china-sea/
[38] Cordova, op. cit., 4
[39] Lyle G Morris. Gray Zone Challenges in the East and South China Sea. (Maritime Issues, 7 January 2019) Accessed 5 April 2021 from http://www.maritimeissues.com/politics/gray-zone-tactics-and-their-challenge-to-maritime-security-in-the-east-and-south-china-sea.html
[40] John Giray. Philippine Cybersecurity. (International Trade Administration, 23 April 2020). Accessed 2 April 2021 from https://www.trade.gov/market-intelligence/philippine-cybersecurity
[41] Miguel Gomez. The Philippines and Cyber Leadership: A Potential Leader. (The Asia Dialogue, 21 April 2017) Accessed 10 May 2021 from https://theasiadialogue.com/2017/04/21/the-philippines-and-cyber-leadership-a-potential-leader/.
[42] Roberto R Romulo. What is the State of Cybersecurity in the Country? (The Philippine Star, 31 January 2020) Accessed 5 May 2021 from https://www.philstar.com/business/2020/01/31/1989079/what-state-cybersecurity-country
[43] Roberto R Romulo. Cyberwar: Is Philippines Defenseless? (The Philippine Star, 17 January 2020). Accessed 26 May 2021 from https://www.philstar.com/business/2020/01/17/1985368/cyberwar-phl-defenseless
[44] Ibid., 2
[45] Ibid., 3
[46] Ibid., 4.
[47] Anton Alifandi. Terrorism in the Philippines: Examining the data and what to expect in the coming years. (Economics & Country Risk Research & Analysis, 09 March 2021). Accessed from https://ihsmarkit.com/research-analysis/terrorism-philippines-examining-data.html
[48] President Papers: The Future of Philippine Warfare, op. cit., 36.
[49] Ibid., 20-21.
[50] Roger Patterson. ISIS "Virtual Caliphate:" What is a Virtual Caliphate? (Justice Clearing House, 18 April 2018). Accessed from https://www.justiceclearinghouse.com/resource/isis-virtual-caliphate-danger-in-our-communities-2/
[51] Op. cit., 25
[52] Hoffman, Conflict in the 21st century: The Rise of Hybrid Wars, op. cit., 39
[53] Ibid., 15.
[54] Antulio J. Echevarria II, "How Should We Think about 'Gray-Zone' Wars?", in Bettina Renz; Hanna Smith, *Russia and Hybrid Warfare – Going beyond the Label*, Report 1/2016, Aleksanteri Institute, University of Helsinki, Finland, pp. 33-39.
[55] Monaghan, op. cit., 92.
[56] President's Paper: The Future of Philippine Warfare, op. cit., 85-86.
[57] Ibid.,
[58] Hoffman. Conflict in the 21st Century: The Rise of Hybrid Wars, op. cit., 58.
[59] Op. cit., 87.
[60] Bastian Giegerich. Hybrid Warfare and the Changing Character of Conflict. (Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, Connections, Vol. 15, No. 2 (Spring 2016), pp. 65-72).
[61] Op. cit., 84.