**Hybrid Warfare**

**Adnan Ali**

**Introduction**

The word Hybrid Warfare has become the new buzzword word which has captured the imaginations and curiosity of people across the globe. For long, countries around the globe had started to document this new method of warfare which deviates from the traditional ways. The different avenues of damage and harm were studied singularly until the early 2000s. Different monikers were used to describe the novel techniques in warfare. Terms like, low intensity war, grey zone tactics, low intensity operations, small wars, irregular warfare, asymmetric warfare, military operations other than wars and others. It became part of the literature in the US in 2006 when it was used by Lieutenant Colonel Frank G. Hoffman of the US Marine Corps[[1]](#footnote-1). Once picked up by the US research groups, the term started to gather importance and its ambit also increased with new damaging techniques clubbed together as weapons of hybrid warfare.

Globalization brought countries together which led to economic and strategic dependence undermining the conventional warfare as aggressive countries were shunned by the rest. However, it created space for hybrid warfare to work around the international systems to avoid any conventional war. Countries continued to work on different methods to sabotage enemies and with new technological advancements more space has been created for hybrid warfare. Tools that can be used to influence countries and institutions are also considered instruments of hybrid warfare. These news tools have violated the jus in Bello[[2]](#footnote-2) principles of warfare: having just cause, last resort, declared by competent authority, right intentions, and reasonable chance of winning, and proportional to means.

The notion of hybrid warfare is not new. The traces of hybrid warfare tactics can be traced to Sun Tzu’s The Art of War. Sun Tzu was a Chinese general, writer and one of the greatest strategist of ancient China whose philosophy of war guided China throughout time. In his book he writes, “The wise warrior avoids the battle”, and “to fight and conquer in all your battles is not supreme excellence, supreme excellence consists of breaking the enemy’s resistance without fighting”[[3]](#footnote-3).

**The Origin and Theory**

As mentioned, different monikers were already in use to describe the new warfare, but the world came upon the term “Hybrid Warfare” after 2006. Hoffman took the term from a thesis done by Robert G Walker in which he explains the low intensity operations of the US marines. In 2006, Hofmann expanded on the idea and called it “complex irregular warfare”. He developed his thesis working with the US marines general. Hofmann first defined hybrid warfare in 2007 in the following words, “Hybrid wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder”[[4]](#footnote-4).

This primary definition was added on multiple times by Hofmann and others. Now, the ambit of hybrid warfare has been stretched enough to include any non-conventional measure to damage countries. The development in the technological space has transformed the warfare methods and has made hybrid warfare more important than ever. Now, media reports, social media platforms, internet of things, Machine learning technologies, international financial institutions, global development agencies, rating agencies, multinational cooperation and other major players are all considered tools of hybrid warfare. These broad inclusions and different monikers with their subtle definitions have been made the term blurry.

After World War II, the term political warfare became synonymous with ambiguous and new conflicts that were beyond the purview of literature ascribed to warfare. Max Boot, American author, took this term from State Department’s memo written by George Kennan, an American Diplomat[[5]](#footnote-5). Other authors have also given credence to political warfare to maximize the US interest with minimum exposure. Kennan had defined political warfare along with lines of economic measures, clandestine support of allies, psychological warfare and encouragement of resistance in hostile states. Hoffman has called political warfare an oxymoron because it does not has any warfare elements, mostly it is political maneuvers[[6]](#footnote-6). Another similar term is hybrid threats used by the US Marine Corps decade ago. This term has been used by the US’ Department of Defense and in their Quadrilateral Defense Review. Recently other terms have also surfaced like “masked warfare” and “new warfare” and then there is Lawfare and Shadow warfare.

Hybrid warfare combines one or more previously defined types of warfare. To clarify the imprecise definition, Hoffman in 2014 called it the not so new warfare in which he defined, “Hybrid threats are any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battlespace to obtain their political objectives[[7]](#footnote-7). It is a mixture kinetic and non-kinetic measures. However, these definitions still do not capture the general current scope that people associate it with.

Another moniker used for hybrid warfare is the fourth generation warfare. William S lind, an American author, distinguishes between the different generations of warfare after the event of Westphalia in 1648 and Daniel H. Abott expanded on it to add the fifth generation warfare[[8]](#footnote-8)[[9]](#footnote-9). First generation warfare worked around organized army, ranks and disciplines against any disorderliness in battle. Second generation warfare introduced new weapons like airplanes, heavy gunfire and artillery. It relied mostly on firepower. Third generation warfare was widely used in World War II and mostly attributed to Germany. It is often associated with warfare of surprise and was led by obedience guided by self-discipline to bypass and undermine the enemy. Fourth generation warfare (4GW) rose to prominence after World War II, it involved non-state actors in warfare. Fifth generation warfare is focused on perceptions and information.

These differentiations by Lind and Abott have added new dimension to war literature which has made strides to make the distinctions clear, but the different monikers continue to complicate the definition and attesting to its hybrid nature. However, these overlapping distinctions certainly fall under the ambit of hybrid warfare which involves one or more warfare techniques to counter the enemy.

**Analysis and Counter measures by NATO**

North Atlantic Treaty Organization (NATO) considers hybrid warfare a threat on my levels and is working assiduously to alleviate its impacts and counter hybrid warfare. NATO believes the primary response to hybrid threats remains with the targeted country. The block has worked on hybrid resilience and is prepared to assist any member state as part of their collective defense pact. The block announced in 2016 that NATO has the power to invoke article 5 of the North Atlantic Treaty if any member state becomes a victim of hybrid attack. Article 5 of the North Atlantic Treaty covers the collective security clause which states that if any member country becomes victim of an attack, each and every other member of the block will consider the attack against all members[[10]](#footnote-10).

Following that in 2018, the block agreed to set up counter-hybrid support teams which were mandated to provide tailored support to allies when requested. The block is working with other stakeholders as well to counter and moderate the threats of hybrid warfare. NATO is stretching out to the European Union as well to assist in counter hybrid threats. The block’s Joint Intelligence and Security Division has analysis unit as well to explain the context of these attacks and provide awareness[[11]](#footnote-11). NATO is working actively to counter misinformation, disinformation, and propaganda with facts.

Cyber threats have become defined feature of hybrid threats along with misinformation and disinformation. NATO’s strategy of prepare, deter, and defend has been put to function and the block is actively working since 2015 on different strategies to counter hybrid warfare[[12]](#footnote-12). NATO’s strategy involves extensive coordination and it is working on it non-NATO states and the EU as well. Beyond EU, NATO is reaching out to partners in Asia-Pacific to counter hybrid threats. NATO worked closely with Ukraine to counter hybrid threats before Russian invasion as their partnership had started in 2016. The European Center for Excellence for Countering Hybrid Threats in Finland provides a platform for expertise, assisting countries in their military and civil capacities, and prepare them to counter hybrid threats. The center has unequivocal support across Europe and NATO. There are other centers adding weight to NATO’s efforts to counter hybrid warfare which include Strategic Communications Center of Excellence in Latvia, the Cooperative Cyber Defense Center of Excellence in Estonia, and the Energy Security Center of Excellence in Lithuania[[13]](#footnote-13).

NATO’s article 3 provides the necessary platform to make member states resilient in face of climate catastrophe, critical infrastructure failure, and hybrid or armed attack. The block is working on the resilience and preparedness to counter hybrid warfare. Preparing the civil space to counter hybrid warfare is a fundamental pillar of country’s resilience[[14]](#footnote-14). The ambit of hybrid warfare is so wide that a single policy will not suffice.

NATO is particularly worried about cyber threats and it is one of the core tasks of collective defense. Cyber threats have become more frequent with the advancement in technology and Europe along with NATO has geared up every possible measure to improve security. A policy was formulated in 2014 which made cyber defense part of the block’s core task of collective defense and NATO affirmed that international law applies in cyberspace. The policy is followed by NATO pledge in 2016 to combat cyber threats. NATO is in extensive coordination with the EU and both have signed Cyber Defense agreement in 2016[[15]](#footnote-15). Regional cooperation amongst countries and stakeholders is very important to prepare and counter cyber threats. Following the importance of cyber space, NATO members supported a new Comprehensive Cyber Defense Policy which endorses NATO’s core tasks.

NATO security complex has grown complicated as the members have agreed on Non-Proliferation of Weapons of Mass Destruction (WMD) and defending the block against Chemical, Biological, Radiological, and Nuclear (CBRN) threats. The block formulated the CBRN policy in 2022 which lays the framework to understand, plan, exercise, train, equip and asses’ capacities across NATO members to counter WMD proliferation and defend against CBRN threats[[16]](#footnote-16).

NATO has comprehensively laid down its framework to counter hybrid warfare threats and to help its member states and allies to moderate its impacts. Hybrid warfare is already active on cyber space where developed countries targeting financial institutions, public records, military assets amongst other vital targets. The focus on research and debate across NATO and allies has added more to the literature of hybrid warfare, but the confusion in its description continues.

NATO along with its allies across the globe is working to minimize the impacts of hybrid warfare on its turf. The affirmation of international laws on cybercrimes and targeted polices on different modes of hybrid threats are vital indications of NATO’s gravity to the hybrid warfare. The developed world enjoys an upper hand over developing worlds. The hybrid threat box of the developed world is different from the developing world which in turn also defines the usage of different hybrid toolkit for defense and offense.

**References**

1. Abbott, D. H. (2010). The Handbook OF 5GW. NIMBLE BOOKS LLC.
2. Hoffman, F. (2014, July 28). On not-so-new warfare: Political warfare vs hybrid threats. War on the Rocks. Retrieved July 13, 2022, from <https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/>
3. Jacobs, J. G. L. J., &amp; Kitzen, M. W. M. (2021, September 22). Hybrid warfare. Oxford bibliographies. Retrieved July 13, 2022, from <https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0260.xml#obo-9780199743292-0260-bibItem-0019>
4. NATO. (2022, June 21). Resilience and civil preparedness – article 3. NATO. Retrieved July 13, 2022, from <https://www.nato.int/cps/en/natohq/topics_132722.htm>
5. NATO. (2022, June 14). NATO's chemical, biological, radiological and nuclear (CBRN) defense policy. NATO. Retrieved July 13, 2022, from <https://www.nato.int/cps/en/natohq/official_texts_197768.htm?selectedLocale=en>
6. Tzu, S. (2010). The art of war [PDF]. Capstone Publishing.
7. Hoffman, Frank G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007.
8. Lind, William S., Keith Nightingale, John F. Schmitt, Joseph W. Sutton, and Gary I. Wilson. “The Changing Face of War: Into the Fourth Generation.” Marine Corps Gazette (October 1989): 22–26.
9. NATO. (2022, June 22). NATO's response to hybrid threats. North Atlantic Treaty Organization, Retrieved July 13, 2022, from <https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text=Since%202015%2C%20NATO%20has%20had,necessary%2C%20will%20defend%20Allies%20concerned>.
10. NATO. (2022, March 23). Cyber defense. NATO. Retrieved July 13, 2022, from <https://www.nato.int/cps/en/natohq/topics_78170.htm>

1. Jacobs, J. G. L. J., &amp; Kitzen, M. W. M. (2021, September 22). Hybrid warfare. Oxfordbibliographies. Retrieved July 13, 2022 [↑](#footnote-ref-1)
2. International humanitarian law, or jus in bello, is the law that governs the way in which warfare is conducted. The rules of jus in bello aim to confine the destructiveness of war, rule out certain kinds of weapons, protect civilians, and limit the area and range of fighting. [↑](#footnote-ref-2)
3. Tzu, S. (2010). The art of war [PDF]. Capstone Publishing. [↑](#footnote-ref-3)
4. Hoffman, Frank G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007. [↑](#footnote-ref-4)
5. Hoffman, F. (2014, July 28). On not-so-new warfare: Political warfare vs hybrid threats. War on the Rocks. Retrieved July 13 [↑](#footnote-ref-5)
6. Hoffman, F. (2014, July 28). On not-so-new warfare: Political warfare vs hybrid threats. War on the Rocks. Retrieved July 13 [↑](#footnote-ref-6)
7. Hoffman, F. (2014, July 28). On not-so-new warfare: Political warfare vs hybrid threats. War on the Rocks. Retrieved July 13 [↑](#footnote-ref-7)
8. Lind, William S., Keith Nightingale, John F. Schmitt, Joseph W. Sutton, and Gary I. Wilson. “The Changing Face of War: Into the Fourth Generation.” Marine Corps Gazette (October 1989): 22–26. [↑](#footnote-ref-8)
9. Abbott, D. H. (2010). The Handbook OF 5GW. NIMBLE BOOKS LLC. [↑](#footnote-ref-9)
10. NATO. (2022, June 22). NATO's response to hybrid threats. North Atlantic Treaty Organization, Retrieved July 13, 2022 [↑](#footnote-ref-10)
11. NATO. (2022, June 22). NATO's response to hybrid threats. North Atlantic Treaty Organization, Retrieved July 13, 2022 [↑](#footnote-ref-11)
12. NATO. (2022, March 23). Cyber defense. NATO. Retrieved July 13, 2022, [↑](#footnote-ref-12)
13. NATO. (2022, March 23). Cyber defense. NATO. Retrieved July 13, 2022, [↑](#footnote-ref-13)
14. NATO. (2022, June 21). Resilience and civil preparedness – article 3. NATO. Retrieved July 13, 2022 [↑](#footnote-ref-14)
15. NATO. (2022, March 23). Cyber defense. NATO. Retrieved July 13, 2022 [↑](#footnote-ref-15)
16. NATO. (2022, June 14). NATO's chemical, biological, radiological and nuclear (CBRN) defense policy. NATO. Retrieved July 13, 2022 [↑](#footnote-ref-16)