Forum: General Assembly 1

Student Officers: Se In Lee, Socorro Ewrine Escalante, Quang Minh Pham

Be sure to consult the UNIS MUN LibGuide for additional resources.

TOPIC 1: The question of limiting hybrid war

I. Introduction to the Topic

Hybrid warfare, by definition, is a form of warfare that fuses both conventional and unconventional instruments and methods in order to exploit the weaknesses of the enemy. Conventional methods consist of traditional weapons, forces, and battlefield tactics. For instance, armored combat vehicles, combat aircraft, warships, ammunition and artillery are all examples of traditional weapons. These weapons are usually paired with regular forces such as infantry and aviation units, as regularly seen in well-known conflicts like World War II. Meanwhile, unconventional weapons and tactics attempt to use irregular instruments of power, including irregular political, economic, civil, international, or cyber tools to undermine antagonists. Such instruments and methods include cyberattacks, disinformation campaigns, diplomatic and economic pressure, and irregular armed forces. A recent example of hybrid warfare in action is the Russo-Ukrainian conflict, where proxy separatist states in Eastern Ukraine (e.g. Donetsk People's Republic, Luhansk People's Republic) and cyberattacks on Ukrainian infrastructure and institutions have and continue to occur alongside Russia's stoppage of gas supplies towards Europe. Russia's usage of private military companies in Libya and Syria. The militant group Hezbollah's usage of modified artillery rockets, media propaganda (e.g. TV Manar, Radio Nour), and terrorist bombings in its conflict against Israel also demonstrates hybrid warfare.

This form of warfare is dangerously efficient, combining conventional and unconventional methods to create synchronized attack packages in order to exploit an enemy's vulnerabilities. Thus, hybrid tactics are extremely efficient since attacks, which are done covertly (secretly) or overtly (openly), could damage various areas and facilitate deniability. Most hybrid warfare tactics and operations could only be limited by its own aggressors, especially with the usage of mass communication, misinformation, or media disruption tactics. Most importantly, hybrid warfare blurs the line between war and peace, since the intensity and efficacy of attacks could be easily controlled, and also damages social order and public morale in populations. This undermines not only governments but also entire societies, creating chaos and thus threatening global peace.

This alarming issue has been addressed in the United Nations, such as in the UN Security Council Open Arria-Formula Meeting on "Hybrid wars as a threat to international peace and security" on March 31, 2017. Nations including the United States and Ukraine highlighted the issue, warning of its threat on global security.

II. Definition of Key Terms

Hybrid warfare: A form of warfare that fuses both conventional and unconventional instruments or methods in order to exploit the weaknesses of the enemy (or antagonist). It is very adaptive because synchronized tactics and methods are constantly changing in novel ways in order to subdue the enemy through all possible means. It is viewed to be dangerous mainly due to its three following abilities:

1. To coerce the enemy without crossing war or detection thresholds;
2. To quickly escalate or de-escalate tensions and carry out damage without forcing a conventional war;
3. To operate covertly and overtly, facilitating actors to deny their actions.

Conventional warfare: A form of warfare that uses conventional weapons and battlefield tactics, which excludes chemical, biological, and nuclear weapons. Primary examples of conventional warfare are World War I and World War II, where armored combat vehicles, combat aircraft, warships, tanks, small arms and light weapons, landmines, cluster munitions, ammunition and artillery were used.

Unconventional warfare: A form of warfare that uses non-military tactics such as cyberwarfare, misinformation/disinformation campaigns, or diplomatic and economic pressure, with the goal of damaging enemies with less costs or risk by exploiting vague war thresholds. Paramilitary groups, non-state actors, and unconventional weapons such as chemical, biological, and nuclear weapons also count under this form of warfare.

MPECI instruments of power: These are military, political, economic, civilian, and informational instruments of power, all of which are commonly used in combinations used in hybrid warfare. Military instruments of power consist of conventional and unconventional weapons and troops; political instruments of power include diplomatic pressure; economic instruments of power include embargoes and sanctions; civilian instruments of power include using civilian knowledge or capabilities to an aggressor's interest; and informational instruments of power include cyberattack operations on infrastructure, organizations, or institutions.

SAPs: an abbreviation for Synchronized Attack Packages, or the combinations of MPECI instruments of power used by aggressors employing hybrid warfare tactics. SAPs are efficient in that they are easily customizable and tailorable to the best of an aggressor's interest, especially in order to attack the vulnerabilities of an enemy.

Instrument of power: all diplomatic, political, military, economic, and informational means available to a government for pursuing a military/political objective.

Tool of subversion: methods or tactics used for weakening or destroying a government, especially through attacks on a population's public morale, social order, or political loyalty towards a national government. This includes cyberattacks, misinformation campaigns, and heavy artillery attacks with psychological purposes.

Non-state actors: Organizations in an armed conflict that are not affiliated with, directed by, or funded by any specific government. They have a variety of uses, ranging from non-military uses (e.g. NGOs providing humanitarian aid) to military uses (violent non-state actors working for their own interest or the interest of a belligerent). In the context of hybrid warfare, non-state actors are mainly criminal organizations (e.g. drug cartels, terrorist organizations, cyberattack organizations) or other violent non-state actors.

III. Key Stakeholders

Russian Federation

The Russian Federation is currently one of the best demonstrators of hybrid warfare as they employ various hybrid tactics in their current armed conflict against Ukraine. They have employed various MPECI instruments of power, including cyber attacks, economic pressure, irregular armed groups, and civilian and political manipulation. In 2014, during the Russian invasion of Crimea, the Russian Federation used "little green men" as part of their invasion strategy. Soldiers without insignia took part in the military operation, thus facilitating Russian deniability. Russia would continue this usage of a paramilitary force in Ukraine by employing the Wagner Group, a Russian private military company known for its pro-Russian operations in Syria, Libya, the Central African Republic, and Venezuela.

At the same time, Russia combined paramilitary forces with cyberattacks on Ukraine, as pro-Russian hackers targeted Ukrainian infrastructure such as power grids, communications systems, electricity systems, and transportation infrastructure; these attacks are also called "cyber fires". From 2014 until May 2022, Russia had been held accountable for 32 major cyber attacks on Ukraine, according to the European Parliament. Misinformation operations targeted at Ukrainian civilians were also carried out as Russia displayed false messages on Ukrainian televisions and also posted a deep fake video of President Volodymyr Zelenskyy surrendering to Russia. Russian hackers also seized sensitive data from

the Ukrainian population, including banking and payment data, citizen credentials, and other sensitive information, which was done to inflict social harm and chaos.

In addition to these cyber operations, Russia also put significant economic pressure on Europe by reducing the flow of the Nord Stream 1 pipeline to one-fifth of its total capacity in July 2022; this pipeline accounts for one-third of Russian gas exports to Europe. This was in reaction to embargoes and sanctions put on Russia by EU and Western countries.

Overall, Russia is one of the most prominent state actors in the hybrid warfare scene, being the only state to actively employ hybrid strategies in a major armed conflict as of this moment. They are closely tied with the Wagner Group, a private military company, and their usage of hybrid tactics are having significant impacts on various regions in the world.

Wagner Group

A Russian private military company (PMC) that is believed to be founded by Yevgeny Prigozhin, a Russian oligarch and close confidant of President Vladimir Putin. The Wagner Group drew global attention after its role in the war in Donbas, Ukraine, where it provided assistance for the separatist states of Donetsk and Luhansk People's Republics in 2014. The group is speculated to also provide troops for Russia in the current Russo-Ukrainian conflict; John Kirby, Coordinator for Strategic Communications at the National Security Council of the White House, estimates Wagner Group has 50,000 soldiers in Ukraine. The group has also been spotted operating for Russian interests in other countries such as Syria, Libya, the Central African Republic, and Venezuela.

This PMC is viewed as a hybrid warfare tool for Russia to facilitate plausible deniability and to hide casualties in armed conflicts, since Wagner soldiers receive military equipment from the Russian Military of Defense and operate in support of Russian interests. Wagner Group is considered as a non-state actor in the hybrid warfare environment, and their existence and operations prove the dangers of hybrid warfare through their facilitation of deniability with their murky organization.

Islamic Republic of Iran

The Iranian Revolutionary Guard and the Iranian government is known for backing the Lebanese political party Hezbollah, which is known for targeting and attacking Israel through hybrid warfare methods such as conventional arsenal, terrorist bombings, and anti-Israeli media propaganda. The act of support and sponsoring of Hezbollah by Iran itself is a demonstration of hybrid warfare, where Iran is employing a non-state actor, in this case a political party or militant group, to inflict harm upon Israel

without directly involving themselves in the conflict and avoiding a direct armed confrontation between the two states. Thus, Iran is one of the few prominent states using known hybrid tactics to a certain level of efficiency.

Hezbollah

A Shiite Muslim political party and militant group based in Lebanon, founded 1982 after the Israeli invasion of Lebanon. They are notorious for their opposition against Israel, use of modified artillery rockets, media propaganda (e.g. TV Manar, Radio Nour), and terrorist bombings. In their opposition against Israel, Hezbollah has been known for having a highly-effective and developed conventional arsenal, possessing a minimum of 100,000 artillery rockets and ballistic missiles. Drawing troops from a large Shia Muslim population in the Middle East, Hezbollah has great manpower that could challenge Israel's security and the security of the Arab region overall. This group poses a very dangerous and long-term threat that should not be ignored.

IV. Key Issues including Background Information

Shift of conflict dynamics

It is clear that aside from blurring the line between war and peace, hybrid warfare is also drastically shifting the dynamics of wars. With rising costs for military development and increasing difficulty in catching up to new military technology, various nations have or will soon be resorting to hybrid warfare for it is low-cost and low-risk while bringing the same, if not even higher efficacy. This is currently being demonstrated by Russia. a country that is consistently employing hybrid tactics due to their lack of military superiority, in the Russo-Ukrainian conflict. Already, complications are noticeable as a result of Russia's novel methods, with Ukraine having to deal with attacks on both the conventional and unconventional fronts, ranging from the physical battlefield to the digital theater. Such expansion in war fronts create vagueness and murkiness for defenders, for adversaries now have a vast array of tools, notably MPECI instruments of power, to fuse together and create specialized-attack-packages (SAPs). Countless possibilities must be explored, calculated, and prepared for by those under attack, and the newly-unlocked fronts pose greater opportunities for a nation to be weakened in various areas. Thus, this shift in dynamics that is redefining warfare will bring devastating security consequences if not prevented or controlled.

Limiting hybrid actors' influence

This is likely the most worrying issue of hybrid warfare, for hybrid tactics now provide a mask for actors to protect themselves, plan operations, and control tensions to their liking, especially with the higher possibility of covert operations. In traditional warfare, any preparations to create a new war front could be easily tracked by various methods including satellites, intelligence, etc. However, unconventional warfare is much more difficult to detect since technological instruments of power could only be detected digitally. This obscurity decreases chances of uncovering covert operations, placing further power into the hands of hybrid actors for they could exploit all instruments of power without any limitations, depriving adversaries of time to develop a proper response before the damage has already been inflicted. Overall, this key issue could create massive power imbalances, greatly shift global political dynamic, and endanger global peace and security.

Digital and social media platforms

With the rise of media platforms, ranging from television to social media applications, nowadays information could be spread quickly worldwide. The speed of digitalized platforms means that misinformation is easy, even under normal circumstances regarding normal topics such as arts or sports. Thus, hybrid actors could utilize this gap to misinform citizens of their adversaries to psychologically decrease public morale, trust, and confidence in populations, damaging the support of citizens for their governments. Some instances of this are the Russian misinformation campaigns done throughout 2022 (e.g. leak of deepfake of President Volodymyr Zelenskyy surrendering on Ukrainian TV). False propaganda is also another threat, as demonstrated by the Al-Manar televisión channel, controlled by the Hezbollah political party to promote anti-Israeli propaganda. Although some campaigns seem subtle and insignificant, they gradually damage the trust between citizens and governments over time by magnifying the magnitude of reported situations and demonstrating governments' weaknesses in certain areas. This bond of trust is of utmost importance, especially in democratic countries, since the people are the backbone of any government and nation; thus, once this bond is broken, social order could collapse completely and countries will fall into chaos, which is the primary objective of hybrid actors.

V. Timeline of Resolutions, Treaties, and Events

Date	Description of event
March 1992	The Israeli embassy in Buenos Aires is bombed in an attack attributed to Hezbollah.
12 July 2006 - 14 August 2006	2006 Lebanon War: Hezbollah demonstrates power of combining unconventional weapons to form hybrid military tactics, using g light anti-tank rocket launchers (RPG-7 and RPG-29) and anti-tank guided missiles (AT-5, AT-13, AT-14 and TOW). 3,790 artillery rockets were used, with a side purpose of imposing a psychological effect on the Israeli population alongside imposing actual military damage.
2012	Hezbollah suicide bombing on a bus with Israeli tourists in Burgas, Bulgaria. This attack was done to impose a psychological impact on the Israeli population, a demonstration of one of the MPECI instruments of power.
2014	Wagner Group enters Donbas, Ukraine to aid the Luhansk and Donetsk's People's Republics. The paramilitary group also sends troops to Crimea in the form of "little green men", or soldiers without insignia working for Russia interests.
2015	Russia deploys its special forces and also enlisted the help of Wagner Group's troops in Syria for its own interest.
13 February 2022	Russia launched a distributed denial-of-service (DDoS) attack on Ukraine, disabling the Ukrainian government, banks, and radio websites for several hours
24 February 2022	On February 24th, 2022, Russia instigated a full invasion of Ukraine.
28 February 2022	Attacks on Ukraine's digital infrastructure disable access to financial and energy resources.
16 March 2022	Televisión channel *Ukraine 24* falsely reports that President Volodymyr Zelenskyy called on the Ukrainian population to surrender after the channel was hacked by Russian hackers
30 March 2022	MarsStealer hacks and gains access to Ukrainian citizens and organizations' user credentials
2 April 2022	Russian hackers steal Ukrainian government officials' user credentials
7 May 2022	Russia launched a cyberattack against Odessa City Council in parallel to a missile attack against Odessa's residential areas

VI. Possible Challenges & Solutions

Vagueness of conflict dynamics

Aware of the obscurity of any incoming hybrid attack from any state, NATO members are constantly sharing and collectively assessing all information attributed to any ongoing hybrid activity. The expansive novel hybrid war fronts also means that preparations for multiple forms of operations are necessary; thus, NATO supports its member states in areas such as "civil preparedness and chemical, biological, radiological and nuclear incident response; critical infrastructure protection; strategic communications; protection of civilians; cyber defense; energy security; and counter-terrorism," according to NATO's official website. This support encompasses the majority of possibilities and SAPs (specialized attack packages) of hybrid warfare.

Limiting hybrid actors' influence

As of this moment, the North Atlantic Treaty Organization (NATO) has proposed several solutions to this mounting issue by using political and military pressure to limit hybrid actors' influence and deter them from further advancing. Since 2016, NATO member states have agreed to invoke Article 5 of the North Atlantic Treaty in the case of hybrid actions against one of more NATO member states; recently, the landing of a reportedly Russian-made missile in Poland raised the possibility of invoking Article 4 of the North Atlantic Treaty, which is a vital step towards invoking Article 5. The invoking of Article 5 would mean that all members would provide armed force assistance to a party or parties under attack if necessary, thus possibly creating an overwhelming alliance against a single adversary.

Digital and social media platforms

NATO has been partnering with the European Union (EU) to counter hybrid threats such as disinformation and propaganda through publication of facts. NATO's Joint Intelligence and Security Division also has a hybrid analysis branch which improves situational awareness of hybrid threats or strategies.

VII. Recommendations for Resolution Writing including Research

First and foremost, delegates must understand their own country's stance on hybrid warfare. Some things to research are the level of threat of hybrid warfare in your country, your country's history of using hybrid tactics, your government's opinions on hybrid warfare, or your country's collaboration with other nations or organizations to either carry out or limit hybrid warfare. Delegates could also search for countries that have tensions with the delegate's country and see if adversaries have used hybrid tactics or methods in the past (on the delegate's country, even). For instance, if the delegate represents the United States, the delegate could research China's and Russia's stances and usage of hybrid warfare methods, while looking towards political allies like NATO and European countries to find commonalities regarding the issue at hand.

Research on adversaries could help delegates form alliances with other countries to craft a resolution; however, it is best to find co-submitters for your resolution by finding nations with simply similar stances on this issue. Other similarities between nations could also include common allies, common adversaries, common policies, etc. Nonetheless, similarities between nations must be in relation to the topic in order to form relevant resolutions.

VIII. Bibliography

Bilal, Arsalan. "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote." *NATO Review*, Nato Review, 30 Nov. 2021, www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

Clark, Mason. "Russian Hybrid Warfare." *Institute for the Study of War*, Institute for the Study of War, Sept. 2020, www.understandingwar.org/report/russian-hybrid-warfare.

"Conventional Weapons." *UNRCPD*, United Nations Regional Centre for Peace and Disarmament in Asia and the Pacific, 13 Dec. 2022, unrcpd.org/conventional-weapons/#:~:text=Conventional%20Weapons%20encompass%20a%20wide,cluster%20munitions%2C%20ammunition%20and%20artillery.

Cullen, Patrick J., and Erik Reichborn-Kjennerud. “MCDC Countering Hybrid Warfare Project: MCDC January 2017 Understanding Hybrid Warfare.” Multinational Capability Development Campaign, Jan. 2017.

Flanagan, Mark, et al. “How a Russian Natural Gas Cutoff Could Weigh on Europe's Economies.” *IMF*, International Monetary Fund, 19 July 202AD, www.imf.org/en/Blogs/Articles/2022/07/19/blog-how-a-russias-natural-gas-cutoff-could-weigh-on-european-economies.

Ganor, Boaz. “CTC-ICT Focus on Israel: What Can We Learn from the Spring 2022 Terror Wave in Israel? .” *CTC Sentinel*, 23 June 2022, ctc.westpoint.edu/wp-content/uploads/2022/06/CTC-SENTINEL-062022.pdf.

“Hezbollah: The Model of a Hybrid Threat - ETH Z.” Edited by Marcin Andrzej Piotrowski et al., *Hezbollah: The Model of a Hybrid Threat*, The Polish Institute of International Affairs, 2 Mar. 2015, www.files.ethz.ch/isn/188946/Bulletin%20PISM%20no%2024%20(756)%202%20March%202015.pdf.

Mackinnon, Amy. “Russia's Wagner Group Doesn't Actually Exist.” *Foreign Policy*, Foreign Policy, 6 July 2021, foreignpolicy.com/2021/07/06/what-is-wagner-group-russia-mercenaries-military-contractor/.

Manko, Oleg, and Yurii Mikhieiev. “Defining the Concept of ‘Hybrid Warfare’ Based on the Analysis of Russia’s Aggression against Ukraine.” *Information & Security: An International Journal*, vol. 41, 2018, pp. 11–20., doi:10.11610/isij.4107.

Nato. “NATO's Response to Hybrid Threats.” *NATO*, North Atlantic Treaty Organization, 22 June 2021, www.nato.int/cps/en/natohq/topics_156338.htm#:~:text=Hybrid%20methods%20of%20warfare%20%E2%80%93%20such,been%20used%20to%20destabilise%20adversaries.

Nato. “The North Atlantic Treaty.” *NATO*, North Atlantic Treaty Organization, 6 Feb. 2019, www.nato.int/cps/en/natolive/official_texts_17120.htm.

Przetacznik, Jakub, and Simona Tarpova. “Russia's War on Ukraine: Timeline of Cyber-Attacks.” European Union, 2022.

“Remarks at a UN Security Council Open Arria-Formula Meeting on ‘Hybrid Wars as a Threat to International Peace and Security.’” *U.S. Department of State*, U.S. Department of State, 31 Mar. 2017, 2009-2017-usun.state.gov/remarks/7733.html.

Steitz, Christoph, and Nina Chestney. “Russia Cuts Gas Flows Further as Europe Urges Energy Saving.” *Reuters*, Thomson Reuters, 27 July 2022, www.reuters.com/business/energy/physical-flows-through-nord-stream-1-pipeline-dip-2022-07-27/.

IX: Additional Resources

“Little green men” in Ukraine. Mainly composed of mercenaries from the Wagner Group, this paramilitary group took part in the Russian invasion of Crimea in 2014. Vasily Fedosenko, Reuters.

A newsroom of an Al-Manar TV station in Beirut, Lebanon. Al-Manar is the television channel of the political party Hezbollah, which is responsible for employing hybrid tactics against Israel, including media propaganda through Al-Manar. (File photo: AP)

Russia has carried various cyber operations against Ukraine, most notably cyber attacks that shut down the Ukrainian power grid in 2015. Valentyn Ogirenko, Reuters.