Study Guide

for

NATO'S North Atlantic Council

Topic Area: Bolstering NATO's hybrid warfare defenses

Table of Contents

1. Welcoming Message

Distinguished Delegates,

It is with great pleasure that we welcome you to NATO's North Atlantic Council (NAC) of RhodesMRC 2022. We feel both honoured and excited to serve as the Board of this iconic committee, especially since 2022 is marked by the return of RhodesMRC as a large, in-person conference.

This year's topic, 'Bolstering NATO's hybrid warfare defence', revolves around today's complicated security environment. Conflicts are no longer primarily waged with military force and are no longer categorized as three different phases of peace, crisis, and conflict. National targets of cyberattacks are those that are not at risk of military attack. Without sending a single army across a single border, social media operations build other worlds that aim to destabilize political communities. Additionally, the "hybrid" combination of military and non-military tools introduces ambiguities that significantly hinder NATO's situational awareness and, as a result, rapid and unanimous decision-making.

In this study guide, we aimed to provide you with all the relevant background information that will help you understand the topic in depth. Additionally, we strived to incentivise you to conduct your own research as well, which is always necessary in order to fully grasp every aspect of a complex international issue. The bibliography and further reading sections at the end of the guide can be great starting points for that research.

On a special note, we kindly want to ask all of you to not only carefully read this study guide, but also the Rules of Procedure (RoP) of NATO's NAC. As familiar as we make ourselves with the topic of the committee, we can never fully shine as delegates without a firm grasp of the rules of the game.

After two very difficult years, during which MUN suffered greatly from the restrictions imposed due to the COVID-19 pandemic, we are really looking forward to meeting each and every one of you in person. Should any questions arise concerning the conference, the committee, the topic or the procedure, feel free to ask for our help and we'll be happy to assist you. On behalf of the Organizing Team and the Secretariat, we welcome you to RhodesMRC 2022 and the island of Rhodes!

Best regards,

Dimitris Lolitsas, Secretary-General of NATO's North Atlantic Council
Alexia Papailiopoulou, Deputy Secretary-General of NATO's North Atlantic Council

2. Introduction to the Committee

2.1. The North Atlantic Treaty Organization

The North Atlantic Treaty Organization (NATO) was established on April 4th, 1949, in Washington, D.C., following the end of World War II. NATO was established as a deterrent of the threat that the Soviet Union posed at the time, as well as a guarantor against chauvinism and aggressive militarism in Europe.[1]

Throughout the Cold War, NATO embraced the doctrine of detention against the Members of the Warsaw Pact. The Alliance broadened its boundaries with the admission of new Member-States and put all its efforts to keep ahead in the arms race with the Soviet Union. Eventually, NATO's strategy against the communist threat paid off, as the dissolution of the Soviet Union marked the end of the Cold War in favour of the West.[2]

The fall of the Berlin Wall on 9 November 1989 seemed to proclaim a new era of open markets, democracy and peace, and the Allies reacted with incredulous joy as emboldened demonstrators overthrew Eastern European Communist governments. But there were also frightening uncertainties. With aggressive chauvinism and militarism in Europe belonging to the past, and the communist threat gone, many questioned the need for the Euro-Atlantic Alliance.[3]

NATO endured because while the Soviet Union was no more, the Alliance's two other initial, if unspoken, mandates still held: to deter the rise of militant chauvinism and to provide the foundation of collective security that would encourage democratisation and political integration in Europe. Several new member States were admissioned and the definition of 'Europe' expanded eastward.

Before the consolidation of peace and security could begin, the issue of coming to terms with a united Germany, which was a permanent concern for European politics since the second half of the nineteenth century, had to be resolved. The incorporation of a re-unified Germany into the Alliance put this most ancient and destructive of dilemmas to rest.

But scepticism around whether NATO had still a place in the global spectrum as a guarantor of peace and security remained. Many voices strongly maintained that the end of the cold war marked the

[1] North Atlantic Treaty Organization (NATO) (2022). 'A short history of NATO'. [online] Available at: https://www.nato.int/cps/en/natohq/declassified_139339.htm [Accessed 5 April 2022]

[2] Encyclopaedia Britannica. 'The Cold War: Toward a new world order'. [online] Available at: https://www.britannica.com/event/Cold-War/Toward-a-new-world-order [Accessed 5 April 2022]

[3] NATO (2022). 'A short history of NATO'. [online] Available at: https://www.nato.int/cps/en/natohq/declassified_139339.htm [Accessed 5 April 2022]

beginning of an era in which the Western Democracies would face no threats to their Liberty and Security, which would lead to an identity crisis of the Alliance.[4]

However, those voices have been proven overoptimistic, as the illegal annexation of Crimea by the Russian Federation in 2014[5], the Syrian conflict[6], and, lately, the Russian invasion of Ukraine[7] have proven to be examples of how important the presence of NATO is. With the dawn of the new decade, the Alliance faces new challenges, as the West's values are once again threatened by totalitarianism.

2.2. The North Atlantic Council

The North Atlantic Council is the principal political decision-making body within NATO. It oversees the political and military process relating to security issues affecting the whole Alliance. It brings together representatives of each member country to discuss policy or operational questions requiring collective decisions, providing a forum for wide-ranging consultation between members on all issues affecting their peace and security.[8]

Decision making

For a decision to be made by the Council, a consensus is required; that means that all member-states have to agree for the decision to pass. In this process, a decision by the majority is not allowed. This need for common acceptance of the Council's decisions means that policies decided upon by the NAC translate the expression of the collective will of all the member states. It is crucial to note that each member has an equal weight in the conversation and all members have equal votes. The Chair of the meetings is the Secretary-General or, in his/her absence, the Deputy Secretary-General.[9]

At the level of permanent representatives, the Council meets every week. A permanent representative voices the views of his/her country, and mainly explains the logic behind the country's policymaking.

[4] Al Jazeera (2021). 'Desperately seeking relevance: NATO in the 21st century'. [online] Available at: https://www.aljazeera.com/features/2021/6/14/desperately-seeking-relevance-nato-in-the-21st-century [Accessed 5 April 2022]

[5] Encyclopaedia Britannica. 'The crisis in Crimea and eastern Ukraine: Russian invasion and annexation of Crimea'. [online] Available at: https://www.britannica.com/place/Ukraine/The-crisis-in-Crimea-and-eastern-Ukraine [Accessed 5 April 2022]

[6] BBC (2016). 'Syria: The story of the conflict'. [online] Available at: https://www.bbc.com/news/world-middle-east-26116868 [Accessed 5 April 2022]

[7] BBC (2022). 'Ukraine war in maps: Tracking the Russian invasion' [online] Available at: https://www.bbc.com/news/world-europe-60506682 [Accessed 5 April 2022]

[8] NATO (2017). 'North Atlantic Council'. [online] Available at: https://www.nato.int/cps/en/natolive/topics_49178.htm [Accessed 5 April 2022]

[9] NATO (2020). 'Consensus decision-making at NATO'. [online] Available at: https://www.nato.int/cps/en/natolive/topics_49178.htm [Accessed 5 April 2022]

The Council can also meet at the level of ministers of Foreign Affairs, ministers of Defence, or even Heads of State/Government.

The Council often publishes declarations and communiqués, which are public documents that explain the Alliance's decisions and reaffirm the Allies' support for aspects of NATO policies.[10]

3. Introduction to the Topic

The modern world has yet to see a more complex and multidimensional term than *'Hybrid Warfare'.* For many, the term under discussion lacks conceptual clarity and is recycling already existing policy debates. Nevertheless, it is with no doubt that 'hybrid warfare' encloses the modern challenges in international defense and security.[11] There is no common ground on the specific interpretation of the term, yet at a first look we could define it as: non-violent subversive actions.[12] However, the complexity of the definition is beyond the term 'non-violent actions'. Currently, the North Atlantic Organization and the European Union (EU) conceive hybrid threats as: military and non-military, conventional and non-conventional, overt and covert actions that can be used by a state or a non-state actor, while remaining out of the traditional concept of war. Despite the common NATO-EU definition, Western politicians usually associate the above-mentioned term with non - violent practices.[13] On the other hand, the United States of America (USA), a very important aspect in formulating international defense and security policy, has used over the years many interpretations, such as*"the diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements acting in concert to achieve mutually benefitting effects".*[14]

The question that follows the problem is nonetheless significant in the introduction to the topic. If there is so much discordance to the interpretation of the term *"hybrid threats"* then there should be even more discordance to the encountering of this matter of security. In other words, if the world cannot

[10] NATO (2022). 'Summit meetings'. [online] Available at: https://www.nato.int/cps/en/natohq/topics_50115.htm [Accessed 5 April 2022]

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

[12] Fri and Tarik SolmazFrom 2014 to 2018, "'Hybrid Warfare': One Term, Many Meanings," 'Hybrid Warfare': One Term, Many Meanings | Small Wars Journal, accessed September 5, 2022, https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings.

[13] *ibid*

[14] The US Department of Army 2019, 1-3

agree on which practices are considered 'hybrid threats', how can we unanimously find an efficient way in eliminating them?

A poor understanding of the concept can lead to the same expansionism that the word 'terrorism' has suffered from, throughout the years. Nowadays "hybrid warfare" has been used to even refer to non-kinetic destabilization operations, complexing the conversation furthermore. To avoid the predicament of the intellectual yet theoretical debate, we will use the common NATO-EU definition of the term, hence without forgetting that there is not such a thing in the world that is not under debate.

4. Key Terms and Definitions

Since finding definitions that the international community agrees upon is almost impossible, this chapter uses the 'NATO Glossary of Terms and Definitions' (AAP-06 Edition 2021)[15] and NATOTerm, the official NATO Terminology Database[16].

- North Atlantic Treaty

  In accordance with Article 6 of the North Atlantic Treaty, the area including the territory of the Parties in Europe and North America and the territory of Turkey, the Mediterranean Sea and the North Atlantic area north of the Tropic of Cancer.

- NATO Body

  A civilian or military headquarters or other organization established pursuant to the North Atlantic Treaty.

- Supreme Allied Commander Europe (SACEUR)

  The NATO strategic commander commanding Allied Command Operations and responsible for the planning and execution of NATO operations.

- Operation

[15] NATO (2021). 'NATO Glossary of Terms and Definitions', AAP-06, Edition 2021. [online] Available at: https://nso.nato.int/nso/zPublic/ap/PROM/AAP-06%202017.pdf [Accessed 5 April 2022]

[16] NATO (2022). 'NATOTerm, The Official NATO Terminology Database'. [online] Available at: https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en [Accessed 5 April 2022]

A sequence of coordinated actions with a defined purpose. Note(s): 1. NATO operations are military. 2. NATO operations contribute to a wider approach including non-military actions.

- NATO-led operation

  An operation utilizing NATO's military structures and incorporating contributions from NATO nations and operational partners, carried out under authority of the North Atlantic Council.

- Operational partner

  A non-NATO country whose contribution of forces, capabilities or other support to a NATO-led operation, has been formally recognized by the North Atlantic Council.

- Security

  The condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion, terrorism and damage, as well as against loss or unauthorized disclosure.

- Mobility

  A quality or capability of military forces which permits them to move from place to place while retaining the ability to fulfil their primary mission.

- Strategic mobility

  The capability to move forces and their associated logistics in a timely and effective manner over long distances. This could be between joint operations areas, between regions, or beyond NATO's area of responsibility.

- Exercise

  A military manoeuvre or simulated wartime operation involving planning, preparation, and execution. It is carried out for the purpose of training and evaluation. It may be a combined, joint, or single service exercise, depending on participating organizations.

- Hybrid threat

  A type of threat that combines conventional, irregular and asymmetric activities in time and space.

- Cyberspace

The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.

- Cyberspace attack (or cyberattack)

  An act or action initiated in or through cyberspace to cause harmful effects.

- Cyberspace operation (or cyberspace op, cyber operation, cyber op)

  Actions in or through cyberspace intended to preserve own and friendly freedom of action in cyberspace and/or to create effects to achieve military objectives.

- Cyber defence

  The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.

- Cyberspace resilience

  The overall technical and procedural ability of systems, organizations and operations to withstand cyber incidents and, where harm is caused, recover from them with no or acceptable impact on mission assurance or continuity.

5. Main Discussion of the Topic

5.1 History of Hybrid Warfare

Peloponnesian War, 431 B.C. Spartans are dedicated to maintaining peace in Laconia and Messenia, their agricultural and military centers. To achieve that they need to prevent an uprising by the Helots who control those centers. Athenians, fully aware of the Spartans' Achilles heel, fortify Pylos with Messenians of Naupactus, whose ancestors the Spartans had expelled from the area after the great Helot uprising of 464 BC. They begin a series of incursions into Laconia, making Helots desert to

Pylos and thus creating a situation of national emergency in Sparta.[17] 2000 years ago, before the word "hybrid" was even created, Athenians were using non-military means to weaken the opponent. During WWII, in the opening phases of Operation Barbarossa, tens of thousands of Soviet partisans created continual disruptions to Germans' lines of communication. During the Second Sino-Japanese War from 1937 to 1945, Mao Tse Tung and his generals were known for using irregular forces to attack not only the Japanese but also his nationalist enemies and the US forces in Korea in 1950 with success even though the Communist forces were clearly outnumbered in all the cases above.[18] The Cold War is known for its hybrid tactics such as propaganda, espionage and embargoes.[19] A brief history of war reveals that hybrid warfare is a significant aspect of every conflict known to history. However, the actual use of the term "hybrid warfare" dates back to the 1990s, first appearing in Thomas Mockaitis' book entitled *British Counterinsurgency in the Post-imperial Era*.[20]

This non-conventional type of war, as the phenomenon called "hybrid warfare", "gained" its worldwide recognition at first in 2008, when the war between Russia and Georgia broke out, with the latter being exposed to severe cyber-attacks.[21] It was no later than 2014 following Russia's invasion of Crimea, when the term finally made it to the political agenda, with NATO using the term to describe the new form of conflict between Russia and Ukraine.[22] NATO's reference did not only bring the term into the spotlight but once again stretched its definition, including from now on, cyber-attacks, economic pressure, and other non-kinetic tools. It seems that it was due to Russia's unconventional strategies that the world was introduced to the military phenomenon called *"hybrid warfare".*

Looking back in history from the Peloponnesian War (431-405 BC) to the American Revolution (1875-1883) and the Vietnam War (1955-1975), every party involved has used irregular tactics to strike the other side. Why is it that now, in the 21st century, the world seems so interested in a phenomenon that has been alive for over 2000 years?

The first element to our structured answer is globalization.[23] Now the geopolitical game is collective, meaning that diplomacy and alliances have a huge impact on international security. From our

[17] Williamson Murray, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (New York, NY: Cambridge Univ. Press, 2012).

[18] *ibid*

[19] "Cold War," Wikipedia (Wikimedia Foundation, August 29, 2022), https://en.wikipedia.org/wiki/Cold_War.

[20] Mockaitis 1995, 14-39

[21] "Hybrid Warfare in Historical Perspectives - NATO Foundation," accessed September 5, 2022, http://www.natofoundation.org/wp-content/uploads/2018/06/NDCF_StefanoMarcuzzi_Paper.pdf.

[22]Fri and Tarik SolmazFrom 2014 to 2018, "'Hybrid Warfare': One Term, Many Meanings," 'Hybrid Warfare': One Term, Many Meanings | Small Wars Journal, accessed September 5, 2022, https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings.

[23] *ibid*

capitalized market and economy to our security and military structure, everything is globalized. With that being said, when Georgia or Ukraine are involved in a hybrid war with Russia, it becomes a matter of global security. This is one of the reasons that the West feels more threatened than it did before.

The second element is technology.[24] "Hybrid" by definition means technology, and with its rapid development hybrid war becomes more advanced, untraceable, more empowered and manipulative towards citizens. The line between peace and war becomes thinner and it creates a new reality where societies are exposed to hybrid threats without comprehending it, thus normalizing it. The new irregular tactics seem to be more powerful than the simple use of arms since not only are they unperceivable to the average person and to the governments themselves, but also because they use all available tools and combine them simultaneously to all levels of warfare.[25] A close-up examination of our history and a prediction of the future indicate that the world is more familiar with hybrid war than we think.

5.2 Forms of Hybrid Warfare

5.2.1. Cyber Warfare

As the world moves onwards to the Fourth Industrial Revolution, where the digital reality and the offline one seem to merge onto each other, all aspects of life are affected, including the way warfare is conducted. Specifically, "war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states[26]" is defined by the term cyber war or cyber warfare. It is based on an [27]information-related principle, in order for the scale of information and knowledge to tip in your favor. The term cyber war should not be assorted with cyberespionage or cybercrime, which is oriented towards illegal ends such as fraud via a computer or a networked device. In most cases, the attack is directed against government and military networks, to disrupt their function or even destroy them completely. The key element to these attacks is the level of knowledge each side has and how it can fortify "[28]its knowledge of itself and its adversaries".

[24] *ibid*

[25] *ibid*

[26] Encyclopedia Britannica. 2022. *cyberwar*. [online] Available at: https://www.britannica.com/topic/cyberwar [Accessed 1 September 2022].

[27] Cyber War is Coming! 1993. Pg 30 [online] Available at: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf [Accessed 1 September 2022].

[28] Cyber War is Coming! 1993. Pg 27 [online] Available at: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf [Accessed 1 September 2022].

The attacks that take place in cyberspace, which constitutes "a virtual world that is created through links between computers, the Internet's infrastructure, servers and routers[29]", can be for [30]intelligence collection, processing and distribution, positioning, IFF (identification-friend-or-foe), for "smart" weapons systems, overloading, intruding into an adversary's information and communications circuits" etc. An adversary can attack all three layers of cyberspace: the physical, the syntactic and the semantic. The first -and crucial- layer is composed of the physical equipment needed, such as hardware, satellites. The second one consists of the software, which is the operating instructions of the first layer. The last one is the human factor (user) that interprets the given information. The form off the attacks can either be physical, by destroying the physical infrastructure or harming the human user, or they can be with weapons such as malware, viruses, spyware, distributed denial-of-service. In regard to the semantic cyberattacks, those are used to [31]alter the users' perception of data in order to obtain key information.

In order to have the proper cyberdefense, the defender has to repeatedly protect its systems and human users, whereas the attacker only needs to succeed once to harm its adversary. A great issue that arises is when a civilian interferes, for such an attack can be instigated by anyone who has the proper knowledge and tools. Furthermore, the anonymity of cyberspace is a great issue for states, for it poses the question of how to combat such attacks.

A well-known case study of cyber warfare is Estonia. In 2007 major cyber-attacks "hit" the country due to the relocation of the "Bronze Soldier Memorial" in Talllinn. Banks, media outlets and government bodies' online services were mostly out of action. Communication in the country was disrupted, journalists could not upload articles to be printed and online banking failed the ordinary citizen. The Russian government [32]denied its involvement, but their position on the matter likely encouraged the culprits, who were most likely individuals with resources. Similar cases are the cyber attacks on Lithuania (2008), Georgia (2008) and Kyrgyzstan (2009).

Cyber defense is also a major part of NATO's [33]core task of collective defence. The main objective is for NATO's networks to be well guarded, to aid Allies in their national resilience and contribute a platform for collective action. Even though the threats are complex, NATO's aim is to continuously

[29] Encyclopedia Britannica. 2022. *cyberspace.* [online] Available at: https://www.britannica.com/topic/cyberspace [Accessed 1 September 2022]

[30] Cyber War is Coming! 1993. Pg 30 [online] Available at: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf [Accessed 1 September 2022].

[31] Encyclopedia Britannica. 2022. *cyberwar*. [online] Available at: https://www.britannica.com/topic/cyberwar [Accessed 1 September 2022].

[32] "Hybrid Threats: 2007 Cyber Attacks on Estonia," StratCom, accessed September 5, 2022, https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

[33] Nato, "Cyber Defence," NATO, July 14, 2022, https://www.nato.int/cps/en/natohq/topics_78170.htm.

evolve and adapt in the new cyber threat landscape. NATO has developed Cyber Rapid Reaction teams to assist Allies when needed, given that they are granted the proper approval. Furthermore, in 2019 the Allies approved of a guide with tools to strengthen the ability to respond to malicious cyber activities. Lastly, in 2021 a new Comprehensive Cyber Defense Policy was endorsed during the NATO Summit in Brussels, which has as its main goal to improve the Alliance's resilience. Each Ally might be responsible for its own cyber defense, but nonetheless NATO aids its members by [34]information sharing through a platform to exchange ways of defense in case of a cyber-attack, by maintaining a rapid- reaction cyber defense team and investing in education, training and exercises.

Finally, NATO engages in various partnerships, such as international organizations, industry, academia and the European Union. At the Madrid Summit, the Allies further agreed that it is of the utmost importance for [35]civil-military cooperation to be strengthened alongside with the industry partnerships. All these actions taken, through cooperation, is how NATO builds a stronghold for all its members, in order to safeguard the liberties that it upholds to the highest standard.

5.3 Misinformation and Disinformation

According to Cambridge's lexicon disinformation is *false information spread in order to deceive people.*[36] NATO ranks disinformation as one of the most characteristic and severe hybrid threats that the world faces. Disinformation alongside fake news and propaganda is widely known as the most powerful form of hostile information activity that threatens democracy. The sole purpose of disinformation is to confuse, manipulate and mislead the population in order to gain control or influence States and their institutions. This phenomenon is as new as war itself, but nowadays due to the rocket use of media, the weaponization of information for military and political gain is easier and more common than ever.[37] According to NATO, and a recent survey of 25 countries, 86% of the population was exposed to disinformation.[38] The 21st century's information landscape finds the world exposed to the threat of disinformation that is mainly being used in the geopolitical game and

[34] "April 2021 NATO Cyber Defence," accessed September 5, 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.

[35] Nato, "NATO and the European Union Work Together to Counter Cyber Threats," NATO, accessed September 5, 2022, https://www.nato.int/cps/en/natohq/news_197959.htm?selectedLocale=en.

[36]"Disinformation," Cambridge Dictionary, accessed September 5, 2022, https://dictionary.cambridge.org/dictionary/english/disinformation.

[37]Nato, "How Does NATO Respond to Disinformation?," NATO, December 21, 2020, https://www.nato.int/cps/en/natohq/news_184036.htm.

[38] Nato, "NATO's Approach to Countering Disinformation," NATO, accessed September 5, 2022, https://www.nato.int/cps/en/natohq/177273.htm.

international relations. According to NATO, there has been an increase in the disinformation's rate since Russia's illegal annexation of Crimea in 2014.

One of the most representative examples is the great scandal of the US elections in 2016. Allegedly, Russia's information warfare affected the US elections in favor of Donald Trump, by creating thousands of social media accounts to urge Americans to vote for the Republican Party and by spreading disinformation through fabricated articles from Russian government-controlled media.[39] This hostile activity that Russia is being accused of leading to economic sanctions against her and closure of Russian diplomatic infrastructures to the US.

As an aspect of hybrid warfare, NATO has developed a strategic policy for countering disinformation, capturing the alliance's dedication to honest communication and transparency.[40]According to the organization, misleading information seeks to divide the allied nations and NATO has been *"facing hybrid challenges, including disinformation campaigns and malicious cyber activities"* as was recognzed in the 2018 Brussels Summit Declaration.[41] To confront the information warfare NATO uses fact-based, credible public communications and a two - aspects approach: understand and engage.[42] The "understand" function analyzes and checks every piece of information relevant to NATO's missions, evaluating the success of its communication. The "engage" function means that the alliance evaluates and tailors its strategy for countering disinformation. Those two functions alongside the understatement of the information environment are crucial parts of NATO's response. Worth mentioning is the NATO Strategic Communications Center of Excellence, which is not a part of the NATO Command Structure but the allies have welcomed its establishment in the 2014 Wales Summit Declaration.

It is significant not to forget that disinformation can be spread by state, and non-state actors, as during the Covid-19 pandemic when NATO became a target of disinformation attacks. In only two days, NATO detected attacks against the presence of its troops in Latvia, Lithuania, and Poland, which included a fake letter, purportedly from NATO Secretary General to the Lithuanian Defense Minister Raimundas Karoblis, stating that the alliance intended of withdrawing the troops, a fake interview claiming that Canadian troops in Latvia had brought the virus to the country, and a forged letter by a

[39] "Russian Interference in the 2016 United States Elections," Wikipedia (Wikimedia Foundation, September 1, 2022), https://en.wikipedia.org/wiki/Russian_interference_in_the_2016_United_States_elections.

[40] Nato, "How Does NATO Respond to Disinformation?," NATO, December 21, 2020, https://www.nato.int/cps/en/natohq/news_184036.htm.

[41] Nato, "NATO's Approach to Countering Disinformation," NATO, accessed September 5, 2022, https://www.nato.int/cps/en/natohq/177273.htm.

[42] *ibid*

Polish military leader appearing to criticize US troops.[43] According to NATO, Russia and the People's Republic of China are the two nations that engage more in disinformation against the West, specifically, since Russia's illegal annexation of Crimea in 2014. Russia's well-known propaganda according to NATO, heated up in 2014, when they invoked the need to protect oppressed Russian minorities living in Eastern Ukraine in order to legitimize the illegal annexation. As Russia's disinformation campaign has elevated after the 2022 invasion - and will be analyzed further down below - so has the response from the West. Worth mentioning is the "Setting the Record Straight" website from NATO, created to narrate the story from the alliance's point of view.[44]

Russia is not the only state accused of spreading disinformation against the West. The People's Republic of China - a close Russian ally and an even closer US frenemy - has a long history of using disinformation campaigns especially according to the situation in Taiwan. Its main goal is to divide the Taiwanian society through disseminating false and deceptive political messages to achieve an annexation, similar to the one in Crimea.[45] Furthermore, many assume that China is Russia's *" most powerful weapon for its information warfare"*, especially after Chinese channels propagated Russia's rhetoric about the situation in Ukraine.[46]

Disinformation is a phenomenon relatively standard as to its definition and meaning. The same statement cannot be used to describe misinformation. Primarily focused on, the most basic difference between those two terms is that disinformation uses a structured campaign in order to spread fake news, while malformation is focused mainly on whether the producer of the malformation has the intention of harming or misleading the audience, in other words, if he is aware that he is spreading fake news.[47] This is the ground and linguistic difference between the two words. Hence, NATO conceives this type of warfare in a more complex way. What turns misinformation from an honest mistake to a part of hybrid warfare is whether the content is manipulative, or whether it can mislead the receiver using several psychological tricks. To sum up the debate, the comparison of the two words, disinformation and misinformation is worth mentioning only on a theoretical level, since in practice, NATO and other major organizations view and treat those two phenomena as two sides of the same coin.

[43] *ibid*

[44] N. "NATO-Russia: Setting the Record Straight." NATO. Accessed September 5, 2022. https://www.nato.int/cps/en/natohq/115204.htm.

[45] https://thediplomat.com/2021/09/chinese-disinformation-operations-what-central-and-eastern-europe can-learn-from-taiwan/

[46] https://www.washingtonpost.com/technology/2022/04/08/russia-china-disinformation/

[47] https://stratcomcoe.org/pdfjs/?file=/publications/download/Inoculation-theory-and-Misinformation-FINAL- dig ital-ISBN-ebbe8.pdf?zoom=page-fit

5.4 Other Methods

5.4.1. Refugees Weaponization

As already mentioned, hybrid warfare is difficult to define. It can be conducted by state or non-state actors and it can use any combination of political, conventional, irregular or cyber warfare. The tactics are numerous, and it would take us a volume to address them all. Hence, having in mind the political chessboard and the ongoing crisis that keeps outbreaking, we should add another dimension to the term "hybrid threat": the weaponization of refugees which is a key factor of unconventional warfare.

It is no hidden secret that we are facing an ongoing refugee crisis due to armed conflicts all around the world, from Syria to Ukraine. Since February 2022, the West has drawn its attention to this crisis because it has, unfortunately, finally reached Europe's doorsteps due to the Russo-Ukrainian War. But the truth is that refugees have been weaponized for centuries and have been used as a pressure and destabilization tool by many governments.

NATO - through its representatives - has been accusing Russia and Syria of utilizing migration to create political instability in Europe, by overwhelming its structures and breaking European resolve.[48] According to the UN, almost 1 million refugees arrived in 2016 in Southern European countries, such as Greece, changing their economic, social, and political givens.[49] For example, the "Barrel Bombs" designed by the Assad government are portrayed from the West as a way to terrorize people and get them out of their homes. *"These indiscriminate weapons used by both Assad and the non-precision use of weapons by Russia, I can't find any other reason for them other than to cause refugees to be on the move and make them someone else's problem",* U.S. Air Force General Philip Breedlove, the supreme allied commander in Europe for NATO stated.[50] The alliance itself does not share a common policy on dealing with this humanitarian crisis, however, it has contributed to dealing with the humanitarian crisis in the Aegean Sea and the Türkiye-Syrian border through intelligence, surveillance, and reconnaissance from NATO's Standing NATO Maritime Group 2 (SNMG2).[51]

5.4.2. Diplomacy

Having elaborated on hybrid threats based on cyber, political, and economic means, it is now time to briefly analyze how diplomacy can turn from a bridge to international relations to a way of meddling

[48] https://www.cnbc.com/2016/03/02/putin-weaponizing-migrant-crisis-to-hurt-europe.html

[49] *ibid*

[50] *ibid*

[51] https://www.nato.int/cps/en/natohq/topics_128746.html

in the decision-making process and boycotting or using the embassies in creating confusing or contradictory narratives.[52] The diplomacy and political domain are strongly connected and so it is only next for the first one to be used as a means to an end for the second one. Often diplomatic sanctions are either invocations to economic sanctions or a way of creating financial instability in the target state. Thus, diplomatic warfare is strongly connected with economic or political warfare and should be examined altogether in order to deeply understand the political structure behind every choice being made.

6. NATO'S Response to Hybrid Challenges

6.1. Hybrid Challenges Require Hybrid Solutions?

NATO has developed a multidimensional policy on countering hybrid threats, focusing mainly on Russia's and China's disinformation campaigns. Hundreds of sites with easy access were created to debunk Russia's allegation about the situation in Ukraine but almost few sites can be found that represent Russia's storyline. Now of course this is the result of the successful coping with Putin's disinformation warfare and it is more than welcome to know that citizens are protected from any effort of manipulation. However, one could not ignore the allegations against the United States and its allies about their interference in hybrid war. Could these allegations be an unconventional effort from the West to counter these unconventional threats? Or are they the proof that hybrid war is a two-way road in the avenue of the geopolitical game?

Till today, numerous and strict sanctions have been imposed not only by NATO and the EU but also from separate governments towards Russia, with the most severe being the one towards Russia's Central Bank, cutting off a fund of roughly $600 billion.[53] The ruble has crashed and the energy market is paralyzed causing a serious economic disaster in every household around the world. Furthermore, the West has proceeded with a cultural and sporting boycott against Russia, leading to the isolation of Russian society. It seems that the West is trying to give Russia a "taste of her own medicine", which is - no matter the cause - doubtful. French finance minister Bruno Le Maire stated that *"We will provoke the collapse of the Russian economy".*[54]This indicates the punitive policy that many governments will adopt but collapsing a country's economy could only lead to the poverty of the population. Thus, the

[52] https://euhybnet.eu/wp-content/uploads/2021/06/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf

[53] https://www.npr.org/2022/03/15/1086641007/without-sending-troops-the-u-s-wages-hybrid-warfare-against- russia

[54] https://www.ft.com/content/ff95ee3f-a1b8-4a54-9657-6a1aaecc105f

real question here is: Do we honestly think that the Russian population is to blame for President Putin's actions?

On the side of the world, the United States competes with the world's second-largest economy, China, in a very fierce way. Pressuring China to ease its “Belt and Roads Initiative” or to revalue its currency against the dollar and the effort to isolate Chinese companies such as Huawei and ZTE from the US market, all indicate that the trade war between the US and China has a huge impact on the political chessboard.[55] Significantly, we should not identify the US with NATO, nonetheless, we should keep in mind that the USA holds the strongest influence within the alliance.

6.2. NATO’s Strategy on Countering Hybrid Threats

State and non-state actors who use hybrid operations to target political institutions, sway public opinion, and jeopardize the security of NATO citizens pose threats to and challenges to NATO Allies. Hybrid forms of warfare, including as sabotage, propaganda, deception, and other non-military strategies, have long been employed to weaken foes. The pace, scope, and ferocity of attacks in recent years have changed, made possible by quick technical advancement and increased worldwide interconnection. NATO has a plan for how it will combat hybrid warfare, and it is prepared to defend the Alliance and all of its allies from any danger, conventional or otherwise. Threats that are hybrid in nature combine military and non-military capabilities as well as covert and overt tactics, such as disinformation campaigns, cyberattacks, economic pressure, the employment of irregular armed groups, and the use of regular forces. In an effort to create doubt in the minds of the target populace, hybrid approaches are utilized to muddy the distinction between war and peace. They seek to weaken and destabilize societies.[56]

NATO has developed a strategy regarding its function in thwarting hybrid warfare since 2015. NATO will make sure the Alliance and its allies are adequately equipped to defend against hybrid strikes in whatever shape they may take. It will discourage hybrid assaults on the Alliance and, if required, defend any affected Allies.[57]

[55] https://thetricontinental.org/red-alert-9-china/

[56] NATO’S Response To Hybrid Threats", NATO, 2022, https://www.nato.int/cps/en/natohq/topics_156338.htm.

[57] Michael Rühle and Clare Roberts, "NATO Review - Enlarging NATO’S Toolbox To Counter Hybrid Threats", NATO Review, 2021, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

NATO regularly collects, shares, and evaluates data **to be prepared** and to identify any ongoing hybrid action. The NATO Headquarters' Joint Intelligence and Security Division enhances the Alliance's comprehension and analysis of hybrid threats. The hybrid analysis branch helps decision-makers become more aware of potential hybrid dangers. If requested, the Alliance will assist Allies in their attempts to determine their own weaknesses and increase their resilience. NATO also acts as a knowledge hub, offering assistance to Allies in a variety of fields, including civil preparedness, CBRN incident response, critical infrastructure protection, strategic communications, civilian protection, cyber defense, energy security, and counterterrorism. In addition to education and training, planning for hybrid threats is extremely important. This entails practicing decision-making techniques and coordinating joint military and non-military responses with other actors.[58]

NATO is determined to act quickly, whenever, and wherever necessary, **to deter** hybrid threats. As part of its deterrent and defense approach, it has upgraded its command structure, decision-making process, and readiness and preparedness of its forces. This strongly suggests that the Alliance is getting better at responding to political and military situations and at deploying the proper forces at the right moment. NATO has also added new tools to its arsenal to combat hybrid threats. Comprehensive preventive and reaction solutions have been established by allies. These choices mix civil and military tools that can be modified to respond to certain circumstances.[59]

NATO is prepared **to defend** any ally against any threat if deterrence should fail. NATO forces must therefore be able to respond swiftly and nimbly whenever and wherever necessary.[60]

6.3. Co-operating with Partners

NATO cannot defeat hybrid threats on its own. Partner collaboration is crucial. To address hybrid threats and improve resilience, the Alliance continues to improve its coordination and collaboration with allies like Finland, Sweden, Georgia, and the European Union (EU). NATO and the EU have increased their collaboration in dealing with hybrid threats as part of their growing partnership, with a particular emphasis on thwarting cyberattacks. Additionally, NATO is collaborating with allies in the Asia-Pacific region to share best practices on national strategies for fending off hybrid threats like the

[58] NATO'S Response To Hybrid Threats", NATO, 2022, https://www.nato.int/cps/en/natohq/topics_156338.htm.

[59] Ibid

[60] Ibid

rise of disinformation campaigns and cyberattacks. This has proven to be especially helpful in relation to the COVID-19 epidemic.[61]

Specifically concerning the relationship of complementarity between EU and NATO, countering hybrid threats is one of the most crucial fields of bilateral cooperation. Naturally, this fact is mirrored in the 2016 Joint Declaration and the reports that followed it: at least 20 out of the 72 common proposals are focused on hybrid threats. This comes as no surprise, since the term 'hybrid threat' encompasses a wide array of incredibly complex and multi-faceted challenges, ranging from combating disinformation and increasing civil preparedness, to countering terrorism and the proliferation of weapons of mass destruction (WMD), and dealing with Chemical, Biological, Radiological and Nuclear (CBRN) issues.[62]

In response to these challenges, NATO and the EU have focused their efforts on coordinating their action in five areas: crisis response, bolstering resilience, situational awareness, strategic communications, and cyber security and defence (which, while a distinct field of cooperation, is still considered 'hybrid' in its nature).[63] When working together, EU and NATO possess a multitude of tools that enable them to successfully detect and counter malicious hybrid activity. Furthermore, the systems at their disposal allow them to render any such activity quite costly to the perpetrator[64], in political, economic and military terms.

With hybrid threats having both civilian and military aspects, which are fundamentally interlinked, the cooperation between the EU and NATO reflects this modern security status quo. The security models of countries like Norway, Sweden, and Finland already point towards that direction, with the first two having adopted a Total Defence concept, which includes a whole-of-society approach to national security and defence issues, utilizing both military and civilian units.

The European Centre of Excellence for Countering Hybrid Threats in Helsinki (HybridCoE), since its establishment in 2017, has been an invaluable tool for EU-NATO cooperation, acting as a neutral space where specialists from the two organizations can work side by side with independent analysts, developing a better understanding of hybrid threats and developing refined solutions on countering

[61] NATO'S Response To Hybrid Threats", NATO, 2022, https://www.nato.int/cps/en/natohq/topics_156338.htm.

[62] European Union External Action (2020). 'EU-NATO cooperation – Factsheet'. [online] Available at: https://www.eeas.europa.eu/sites/default/files/eu_nato_factshee_november-2020-v2.pdf [Accessed 5 April 2022]

[63] Zandee D., Van der Meer S., Stoetman A. (2021). 'Countering hybrid threats. Steps for improving EU-NATO cooperation'. Netherlands Institute of International Relations 'Clingendael'. [online] Available at: https://www.clingendael.org/pub/2021/countering-hybrid-threats/ [Accessed 5 April 2022]

[64] Smith H. (2021). 'Countering hybrid threats', ed. Lindstrom G., Tardy T., *The EU and NATO – The Essential Partners.* European Union Institute for Security Studies (EUISS). [online] Available at: http://publications.europa.eu/resource/cellar/08e9e07b-cd30-11e9-992f-01aa75ed71a1.0001.01/DOC_1 [Accessed 5 April 2022]

them. At the same time, the informal networks that are created through this process complement the formal ones, making crucial information sharing easier, faster and more efficient[65].

Cyber security and defence is one of the main pillars of the cooperation between NATO and the EU, underlining the importance of cyberspace in today's digital age security environment. The two organizations and their member states face similar cyber threats that undermine both civil and military security, often including political and economic aspects. Especially during the last two decades, the rapid increase of cyberspace attacks, along with the high level of reliance on various digital systems, has pushed NATO and the EU to adopt common policies regarding their cyberspace resilience, consulting each other and coordinating their efforts.[66] Particularly, the 2014 Russian invasion of Crimea also included a number of sophisticated cyber operations, namely denial-of-service attacks (DDoS), which devastated a large number of websites and systems.[67] In the aftermath of that, the looming and imminent danger of cyberattacks led to an exponential increase in common cyber defence initiatives by the two organizations.

In the field of cyber concepts and doctrines, several exchange activities have taken place, including joint workshops, cross-briefings and training and education courses.[68] These activities were carried out at varying levels, with regular Working Groups and Committee meetings being supplemented by high-level staff talks and joint participation in cyber exercises.[69] An important result of these exchanges was the formation of a platform, where all mutually beneficial ideas and documents could be reviewed and explored, with regard to their realisability and potential for development.[70]

In February 2016 NATO and the EU signed a Technical Agreement on Cyber Defence, enabling operational-level information sharing between the NATO Computer Incident Response Capability (NCIRC) and the EU Computer Emergency Response Team (CERT-EU). Another important step is the fact that since 2017 the main crisis management exercises conducted by NATO and the EU,

[65] Ibid

[66] Lété B., (2021). 'Cooperation in Cyberspace', ed. Lindstrom G., Tardy T., The EU and NATO – The Essential Partners. European Union Institute for Security Studies (EUISS). [online] Available at: http://publications.europa.eu/resource/cellar/08e9e07b-cd30-11e9-992f-01aa75ed71a1.0001.01/DOC_1 [Accessed 5 April 2022]

[67] Ibid

[68] Zandee D., Van der Meer S., Stoetman A. (2021). 'Countering hybrid threats. Steps for improving EU-NATO cooperation'. Netherlands Institute of International Relations 'Clingendael'. [online] Available at: https://www.clingendael.org/pub/2021/countering-hybrid-threats/ [Accessed 5 April 2022]

[69] European Union External Action (2020). 'EU-NATO cooperation – Factsheet'. [online] Available at: https://www.eeas.europa.eu/sites/default/files/eu_nato_factshee_november-2020-v2.pdf [Accessed 5 April 2022]

[70] NATO – EU (2020). 'Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017'. [online] Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf [Accessed 5 April 2022]

called EU PACE and NATO CMX respectively, are being held simultaneously and in a coordinated manner, allowing for the mutual participation of EU and NATO officials and specialists.[71] The man framework for cyberspace cooperation was laid out in the 2016 and 2018 Joint EU-NATO declarations, which underlined the importance of understanding and improving the synergies between the EU and NATO[72].

7. Hybrid Warfare and Article 5 of the North Atlantic Treaty

Member states' core promise to the alliance is guaranteed in article 5 of the North Atlantic Treaty which states that *"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently, they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area".* This article and the whole treaty itself were drafted in a time when only kinetic means were known and used in armed conflicts. The rise of hybrid threats raised the very important question: Could any form of hybrid warfare trigger article 5? When it comes to diplomatic, financial, or political warfare the answer is quite simple and justifiable. A simple diplomatic episode or an embargo could not possibly trigger the collective defense.

The breakthrough came in 2014 at the Wales Summit where the Declaration recognized the possibility for a cyber attack to trigger the implementation of article 5 based on the effect and magnitude of the attack. From the very first reference, the alliance made it clear that a cyber attack could trigger article 5 and the only question left to answer was "when". The same conclusion was reached in the Warsaw Summit Communique, where NATO declared cyberspace as a new operational domain next to land, sea and air and in the Brussels Summit Communique. The key element was a case by case examination in order to evaluate if the invocation of article 5 would be necessary. Eventually. NATO

[71] Lété B., (2021). 'Cooperation in Cyberspace', ed. Lindstrom G., Tardy T., The EU and NATO – The Essential Partners. European Union Institute for Security Studies (EUISS). [online] Available at: http://publications.europa.eu/resource/cellar/08e9e07b-cd30-11e9-992f-01aa75ed71a1.0001.01/DOC_1 [Accessed 5 April 2022]

[72] Ibid

has stated that the same policy applies to all forms of hybrid warfare and if someone visits their website, they will read the same policy loud and clear.[73]

What is not loud and clear is the line between a simple cyber attack and one that could invoke article 5. Jens Stoltenberg, NATO's Secretary-General has stated that both the extent of such an attack and the Allied response under Article 5 '*must remain purposefully vague*'. However, the alliance has stated that if attacks such as the one to Estonia in 2007 could trigger NATO's collective defense.

To summarize both hybrid and cyber attacks could lead to the implementation of article 5, hence this statement should be conceived with thriftiness and always under consideration of the circumstances. Let us not forget that NATO has a long history of escalating its responses to a threat, meaning that first of all political, diplomatic, and economic means shall be exhausted before choosing a solution that would end up in World War III. [74]

8. The War in Ukraine and Hybrid Challenges

The most breaking news of 2022 was the Russian invasion in Ukraine on February 24. While this invasion is based 100 percent on conventional military means, the truth is that the war between the two countries has been ongoing for many years. What changed on February 24, was just the means. The hybrid challenges that Ukraine has been facing since almost 2014, are the reason that the term "hybrid warfare" entered the military lexicon. It is the most overwhelming example of the topic under discussion and we will delve into it to get a better understanding of the challenges that NATO faces.

8.1. Cyber Attacks

Viktor Zhora, deputy chairman of the State Service of Special Communications in Ukraine reports that Ukraine is fighting on two battlefields: the conventional armed conflict and the cyber-war that Russia has abolished. Allegedly, his country has been facing constant cyber attacks from Russia since 2015, such as "wiper attacks" that removed data from a Ukrainian private company or power cuts in small cities. Ukraine has responded to the threats in a controversially way by launching an "IT Army of

[73] https://www.nato.int/cps/en/natohq/topics_156338.htm

[74] https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/

Ukraine", which has been carrying out cyber-attacks on Russian targets, such as attempts to disrupt transport and power networks.[75] While Ukrainian officials claim that no attacks are against citizens but only against the government and military, it is at least peculiar that a state officially admits to cyber attacking another country. In April 2022, Ukrainian officials reported that they have intercepted a Russian cyber attack on their electric grid that would have paralyzed almost all of western Ukraine by shutting down all communications, electricity, emergency services, and other crucial infrastructures.[76] Considering the technological capabilities that Russia has and comparing them with Ukraine, a much smaller nation, it comes with a surprise that most of the cyber attacks on Ukraine are inefficient. The close cooperation with NATO has offered Ukraine the opportunity to defend itself efficiently against attacks and enhance its cyber security policy.

NATO has openly stated many times that it condemns the cyber attacks against Ukraine and they are working alongside to boost Ukraine's cyber security system. At the NATO Summit in Madrid, the alliance announced an even closer collaboration in the cyber defense field by providing an additional cyber security trust fund. Last August, Ukraine announced that its National Cyber Security Strategy will integrate with NATO's cyber defense system in order to exchange knowledge and scientific data and to provide the necessary training and personnel. On January 17, 2022, NATO Communications and Information Agency (NCIA) and president Zelensky renewed a Memorandum of Agreement to maintain cooperation in technology-related projects and to modernize Ukraine's defense capabilities.[77]

Considering how successful the NATO-Ukrainian collaboration is in the cyber security field, many experts are voicing their concerns that Russia might turn its cyber attacks against a NATO ally.

8.2. Disinformation

One of the strongest hybrid threats that Russia uses is the disinformation campaigns against Ukraine with the purpose of spreading propaganda and legitimizing the invasion. Russia claims that the Russian minorities in Dombas are in danger because the Ukrainian government is using neo-nazi armed groups to commit genocide against them. Russian propaganda includes manufacturing videos and photographs to deepfake, closing all independent media and prohibiting any anti-war speech.

[75] https://www.bbc.com/news/technology-60622977

[76] https://gjia.georgetown.edu/2022/08/08/cyberattacks-and-the-russian-war-in-ukraine-the-role-of-nato-and-risks-of-escalation%EF%BF%BC/

[77] https://www.eurointegration.com.ua/eng/news/2022/07/6/7142685/

Meanwhile in Melitopol, one of Russia's first successes in Ukraine, Russian broadcasts had replaced their local radio; one played a speech by Putin on a loop and soldiers posted flyers that declared the fighting was for "the defense of Russia itself from those who have taken Ukraine hostage" and called for "cooperation so that we can quickly turn this tragic page and move forward together", according to "*Times*". [78]

While the Western internet is convinced about Russia's fault in the war, we cannot state the same about the controlled internet in countries such as China, Turkiey, and India. Zero countries from the Middle East and South America have imposed sanctions on Russia. According to the Economist Intelligence Unit, two-thirds of the world's population live in countries that are neutral about the war or support Russia. China is an open ally to Russia, but many other countries such the United Arabes Emirates, South Africa, and Brazil refuse to criticize Putin and are willing to share Russia's informations about the war in the media. Apparently, the two most popular hashtags in India are #IStandWithPutin and #IStandWithRussia. The new protagonist is Telegram, an encrypted platform that Zelensky is using to address the Russians and Putin is using it to address the Ukrainians.

To argue that Ukraine is winning in information warfare would be a false statement. The West alongside NATO is dedicated to bringing down Russian propaganda and they are achieving it when it comes to the area of the internet that is under their control. However, there is still a large part of the world where the West holds little to non-influence, and that part of the world is probably leaning toward Russia, meaning that at the end of the day, Putin has launched a successful disinformation campaign.

Yet, Putin is still struggling to gain power over Europe which is after all a highly important region for Russia. Is it possible for Russia to use its hybrid tactics against the West or any other NATO ally? The risk of escalation is not as far as someone might think it is. After all, a brief flashback to 2017 will remind us of the NotPeya incident, where Russia attacked Ukrainian targets, yet a simple malfunction in the malware caused the misdirection of the attack resulting in 10 billion dollars in commercial harm to Western campaigns.[79]As many hybrid threats, Russia decides to unleash against Ukraine just as many sanctions the West will continue imposing targeting Russia's economy feeding the circle of escalation between the two sides. On April 15, 2022, Putin warned of "unpredictable consequences" if the West continued with its punitive policy. The tension is rising as the days go by and the fallouts

[78] https://www.newsweek.com/putin-bringing-his-disinformation-war-ukraine-1708674

[79] Serena Liu, "Cyberattacks and the Russian War in Ukraine: The Role of NATO and Risks of Escalation," Georgetown Journal of International Affairs, August 7, 2022, https://gjia.georgetown.edu/2022/08/08/cyberattacks-and-the-russian-war-in-ukraine-the-role-of-nato-and-risks-of-escalation%EF%BF%BC/.

of this irregular conflict are left to be narrated in history books. Till then, NATO is charged with finding new hybrid ways to win another round of the hybrid game.

9. Conclusion

Back in the 1980s, when the world could only imagine the tremendous technological developments, the most horrific consequence they could have thought of was that robots would somehow take over the world and rule humanity. Who could have pictured the idea that the most modern challenges of global peace would be based on common - everyday tools such as information, currency, the internet, and eventually, human beings? From the 1980s till today, from science-fiction to reality, hybrid warfare has well earned its place in the timeline of modern conflicts. Since modern problems require modern solutions, the North Atlantic Council has developed a detailed and specialized plan for deterring hybrid threats that consists of three important steps: prepare, deter, and defend. From analyzing hybrid threats in the NATO Headquarters' Joint Intelligence and Security Division to creating new forms of defense such as comprehensive preventive and reaction solutions, NAC has proved to be one of the few decision-making bodies that are efficiently prepared against hybrid warfare. Nonetheless, the Madrid Summit is the most concrete proof that the alliance is always evolving and adjusting to the constantly changing field of hybridity. Hence, regardless of the power that NATO holds, it remains above all an alliance, which was created in order to work alongside others. One of the strongest allies, the EU, is the key factor in NATO's policy on countering disinformation and cyber-attacks and it would be no exaggeration to state that only with the close cooperation of the two international organizations, the world could isolate these threats. Considering that the conventional war is now closer in Europe than it has ever been in many years and that the "heart" of hybrid war is in its territories, it is necessitated to focus our efforts on Europe's fortification. With this information in our minds, we have opened up new dimensions in the term "collective defense", dimensions that could either lead to unity and prosperity, or to World War III -if we choose to believe that we are not already experiencing WWIII -. Is the world ready to face the consequences of its own construction? Or is it doomed to a vicious circle between development and disaster?

10. Points to be Addressed

1. Why is cyber warfare one of the most dangerous forms of cyber defense and how can the alliance protect itself from it?
2. Should NATO continue offering its support to the Ukrainian defense system, risking in that way a potential hybrid attack from Russia? How can NATO maintain its cyber - partnership with Ukraine while simultaneously protecting itself from such threats?
3. In which ways the alliance could bolster its campaign against disinformation and misinformation without violating the right to free speech?
4. How can NATO - a military alliance - contribute to the elimination of the refugees' weaponization?
5. Which should be the criteria for activating Article 5 when an ally is under hybrid attack? How would NATO respond if an ally were to use hybrid warfare against another ally?
6. Could the severe economic pressure be considered a form of attack against one nation? How can NATO protect its less developed members from the severe consequences of economic pressure?
7. How can Europe protect itself from Russia's hybrid warfare and which could be NATO's contribution?
8. What is the most efficient response to hybrid threats?

11. Further Reading

1. Kim Wijnja (2022) Countering hybrid threats: does strategic culture matter?, Defence Studies, 22:1, 16-34, DOI: 10.1080/14702436.2021.1945452
2. Silvie Janičatová & Petra Mlejnková (2021) The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities, Contemporary Security Policy, 42:3, 312-344, DOI: 10.1080/13523260.2021.1885921
3. Clingendael.Org, 2022. https://www.clingendael.org/sites/default/files/2021-10/countering-hybrid-threats.pdf.
4. R. Craig Nation Dr. and Michael McFaul Dr., The United States and Russia into the 21st Century (US Army War College Press, 1997) https://press.armywarcollege.edu/monographs/179

5. David J. Lonsdale (2020) The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios, Journal of Military Ethics, 19:1, 20-39, DOI: 10.1080/15027570.2020.1764694

12. Bibliography

- "A Short History Of NATO". NATO, 2022. https://www.nato.int/cps/en/natohq/declassified_139339.htm.
- Admin. “Red Alert: The US-Imposed Hybrid War on China.” Tricontinental, September 23, 2020. https://thetricontinental.org/red-alert-9-china/.
- “April 2021 NATO Cyber Defence.” Accessed September 5, 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf
- Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!". Rand.Org, 2007. https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf.
- Bachulska, Alicja, and Lin Pu. “Chinese Disinformation Operations: What Central and Eastern Europe Can Learn from Taiwan.” – The Diplomat. for The Diplomat, September 24, 2021. https://thediplomat.com/2021/09/chinese-disinformation-operations-what-central-and-eastern-europe-can-learn-from-taiwan/.
- “Building a Comprehensive Approach to Countering Hybrid Threats ... - NATO.” Accessed September 13, 2022. https://nmiotc.nato.int/wp-content/uploads/2020/02/Building-a-Comprehensive-Approach-to-Countering-Hybrid-Threats-in-the-Black-Sea-and-Mediterranean-Regions-by-Chris-Kremidas-Courtney.pdf.
- Bilal, Arsalan. “Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote.” NATO Review. Nato Review, November 30, 2021. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.
- “Cold War.” Wikipedia. Wikimedia Foundation, August 29, 2022. https://en.wikipedia.org/wiki/Cold_War.
- "Cold War - Gorbachev and The Reunification Of Germany". Encyclopedia Britannica, 2022. https://www.britannica.com/event/Cold-War/Toward-a-new-world-order.
- "Consensus Decision-Making At NATO". NATO, 2022. https://www.nato.int/cps/en/natolive/topics_49178.htm.

- “Cyber Attacks and Article 5 – a Note on a Blurry but Consistent Position of NATO.” CCDCOE. Accessed September 14, 2022. https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/.
- "Cyber Defence". NATO, 2022. https://www.nato.int/cps/en/natohq/topics_78170.htm.
- "Cyberspace | Communications". Encyclopedia Britannica, 2022. https://www.britannica.com/topic/cyberspace.
- "Cyberwar". Encyclopedia Britannica, 2022. https://www.britannica.com/topic/cyberwar.
- “Disinformation.” Cambridge Dictionary. Accessed September 5, 2022. https://dictionary.cambridge.org/dictionary/english/disinformation.
- Dwoskin, Elizabeth. “China Is Russia's Most Powerful Weapon for Information Warfare.” The Washington Post. WP Company, April 10, 2022. https://www.washingtonpost.com/technology/2022/04/08/russia-china-disinformation/.
- Ellyatt, Holly. “Putin 'Weaponizing' Migrant Crisis to Hurt Europe.” CNBC. CNBC, March 2, 2016. https://www.cnbc.com/2016/03/02/putin-weaponizing-migrant-crisis-to-hurt-europe.html.
- "EU-NATO Cooperation". EEAS, 2020. https://www.eeas.europa.eu/sites/default/files/eu_nato_factshee_november-2020-v2.pdf.
- European Pravda. “Ukraine Cooperates Closer with NATO on Cyber Defense.” Ukraine Cooperates Closer with NATO on Cyber Defense. European Pravda, July 6, 2022. https://www.eurointegration.com.ua/eng/news/2022/07/6/7142685/.
- "Fifth Progress Report On The Implementation Of The Common Set Of Proposals Endorsed By EU And NATO Councils On 6 December 2016 And 5 December 2017". NATO & EU, 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf.
- Fri, and Tarik SolmazFrom 2014 to 2018. “'Hybrid Warfare': One Term, Many Meanings.” 'Hybrid Warfare': One Term, Many Meanings | Small Wars Journal. Accessed September 5, 2022. https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings.
- Gatopoulos, Alex. "Desperately Seeking Relevance: NATO In The 21St Century". Aljazeera.Com, 2021. https://www.aljazeera.com/features/2021/6/14/desperately-seeking-relevance-nato-in-the-21st-century.
- “Hybrid Warfare in Historical Perspectives - NATO Foundation.” Accessed September 5, 2022. http://www.natofoundation.org/wp-content/uploads/2018/06/NDCF_StefanoMarcuzzi_Paper.pdf.
- “How Does NATO Respond to Disinformation?” NATO, December 21, 2020. https://www.nato.int/cps/en/natohq/news_184036.htm.
- Jackson, Jon. “Putin Is Bringing His Disinformation War to Ukraine.” Newsweek. Newsweek, May 20, 2022. https://www.newsweek.com/putin-bringing-his-disinformation-war-ukraine-1708674.

- Lété, Bruno, Gustav Lindstorm, and Thierry Tardy. "Cooperation In Cyberspace". The EU And NATO | The Essential Partners, 2019. http://publications.europa.eu/resource/cellar/08e9e07b-cd30-11e9-992f-01aa75ed71a1.0001.01/DOC_1.
- Liu, Serena. “Cyberattacks and the Russian War in Ukraine: The Role of NATO and Risks of Escalation.” Georgetown Journal of International Affairs, August 7, 2022. https://gjia.georgetown.edu/2022/08/08/cyberattacks-and-the-russian-war-in-ukraine-the-role-of-nato-and-risks-of-escalation%EF%BF%BC/
- Murray, Williamson. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. New York, NY: Cambridge Univ. Press, 2012.
- Myre, Greg. “Without Sending Troops, the U.S. Wages 'Hybrid Warfare' against Russia.” NPR. NPR, March 15, 2022. https://www.npr.org/2022/03/15/1086641007/without-sending-troops-the-u-s-wages-hybrid-warfare-against-russia.
- “NATO and the European Union Work Together to Counter Cyber Threats.” NATO. Accessed September 5, 2022. https://www.nato.int/cps/en/natohq/news_197959.htm?selectedLocale=en.
- “NATO's Approach to Countering Disinformation.” NATO. Accessed September 5, 2022. https://www.nato.int/cps/en/natohq/177273.htm.
- “NATO's Response to Hybrid Threats.” NATO, June 22, 2021. https://www.nato.int/cps/en/natohq/topics_156338.htm.
- "NATO And The European Union Work Together To Counter Cyber Threats". NATO, 2022. https://www.nato.int/cps/en/natohq/news_197959.htm?selectedLocale=en.
- “NATO Chief Warns against Trading Security for Economic Interests.” Anadolu Ajansı. Accessed September 14, 2022. https://www.aa.com.tr/en/europe/nato-chief-warns-against-trading-security-for-economic-interests/2596301.
- "North Atlantic Council (NAC)". NATO, 2022. https://www.nato.int/cps/en/natohq/topics_49763.htm.
- Rühle, Michael and Roberts, Clare. "NATO Review - Enlarging NATO’S Toolbox To Counter Hybrid Threats". NATO Review, 2021. https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.
- “Russian Interference in the 2016 United States Elections.” Wikipedia. Wikimedia Foundation, September 1, 2022. https://en.wikipedia.org/wiki/Russian_interference_in_the_2016_United_States_elections.
- “Security and Defence Quarterly - Online First Articles.” Security and Defence Quarterly - Online first articles. Accessed September 14, 2022. https://securityanddefence.pl/.

- Smith, Hanna, Gustav Lindstorm, and Thierry Tardy. "Countering Hybrid Threats". The EU And NATO | The Essential Partners, 2019. http://publications.europa.eu/resource/cellar/08e9e07b-cd30-11e9-992f-01aa75ed71a1.0001.01/DOC_1.
- "Stratcom | NATO Strategic Communications Centre Of Excellence Riga, Latvia". Stratcomcoe.Org, 2019. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.
- "Summit Meetings". NATO, 2022. https://www.nato.int/cps/en/natohq/topics_50115.htm.
- "Syria: The Story Of The Conflict". BBC News, 2016. https://www.bbc.com/news/world-middle-east-26116868.
- Tidy, Joe. “Ukraine Says It Is Fighting First 'Hybrid War'.” BBC News. BBC, March 4, 2022. https://www.bbc.com/news/technology-60622977.
- "Ukraine - The Crisis In Crimea And Eastern Ukraine". Encyclopedia Britannica, 2022. https://www.britannica.com/place/Ukraine/The-crisis-in-Crimea-and-eastern-Ukraine.
- "Ukraine War In Maps: Tracking The Russian Invasion". BBC News, 2022. https://www.bbc.com/news/world-europe-60506682.
- Wigglesworth, Robin, Colby Smith, and Claire Jones. “The West's Hybrid War on Russia.” Financial Times, March 4, 2022. https://www.ft.com/content/ff95ee3f-a1b8-4a54-9657-6a1aaecc105f
- Zandee, Dick, Sico van der Meer, and Adája Stoetman. "Countering Hybrid Threats". Clingendael.Org, 2021. https://www.clingendael.org/pub/2021/countering-hybrid-threats/.