

Committee: Disarmament and International Security Committee (GA1)

Issue: Responding to hybrid threats and asymmetric warfare

Student Officer: Antonis Chronis

Position: Co-Chair

INTRODUCTION

The international security environment has entered a new era in the perception of war and peace, departing from a post-cold war period. In the past years, the security issues and challenges arising from hybrid threats as well as wars have ruled the security agendas of the international community resulting in international concerns.

Nevertheless, it is widely known that despite the attention that has been brought to the issue of “hybrid threats and asymmetric warfare”, there is a clear lack of information concerning how these fairly new phenomena should be handled and dealt with. While studies are to be seen on specific issues, an effective approach to how hybrid wars and threats are to be handled is still lacking.

The aforementioned issue has been recognised by both the European Union and the North Atlantic Treaty Organization, which have made efforts to precisely define the term “hybrid threat” in order to effectively tackle it, but have not reached a conclusion.

It should be, at this point, mentioned that the international community has considered the issue of asymmetric warfare of utmost concern since it has become a strategy, which is mostly preferred by dissident, extremist political groups. Operating secretly in no sovereign territories, parties using asymmetric strategies have been engaging in lethal and violent activities with far less risk of being totally taken aback by reprisals that a nation-state might face.

Thus, it is crucial to mitigate the impact of hybrid threats and asymmetric warfare, taking into consideration that their use is more than capable of causing huge destruction. Hence, it is vital to develop new legal frameworks and ways of limiting the use of such military offensives. Relying on conventional military strategies is an inadequate way to counter what has finally evolved into a totally unfamiliar national and, indeed, global security threat as

shown by the Soviet interventions in Afghanistan and the abortive Israeli attack on Hezbollah (2006).

DEFINITION OF KEY TERMS

Hybrid Threat

Hybrid threats are activities or methods that aim to target vulnerable areas of the opponent party. Under the term “vulnerabilities” lie factors such as the historical background of a state, its legislation, potential old practices, a strong polarisation of society, technological issues as well as geostrategic factors.

Asymmetric Warfare

Asymmetric warfare occurs when military practices adopting different means take place. Such practices are often characterised by the use of unconventional weapons and activities. Through the term asymmetric warfare, it is understood that the opposing forces differ greatly in their military power and forces. This military strategy can be often used with the term “guerilla warfare”.

Economic Warfare

Economic warfare can be considered as a form of a hybrid threat since it involves the implementation of economic means such as the imposition of tariffs or sanctions against a state, an organization or an individual. Economic warfare can escalate, in extreme cases, to an economic embargo which would completely damage a nation’s trade relations or financial status.

BACKGROUND INFORMATION

History of hybrid and asymmetric warfare

Although being fairly new military offensives, the use of hybrid and asymmetric warfare traces back several centuries. Such have been taking place as long as nations or ethnic groups started operating militarily to expand their territories. These methods have existed since ancient times (that is, the Trojan war which was concluded with the invasion of the Greeks through the use of the Trojan Horse) but their involvement becomes more visible during the early 2000s.

The Hezbollah attacks

The war between the Israeli government and Hezbollah (2006) is often referred to as the prototype of hybrid wars in recent history. During the escalation of the conflict, Hezbollah displayed all of the elements that engage in a hybrid threat: "... the simultaneous use of a conventional arsenal, irregular forces and guerrilla tactics, psychological warfare, terrorism and even criminal activities, with support from a multidimensional organization and capable of integrating very different sub-units, groups or cells into one united, large force."¹

Assisted by Iran, Hezbollah armed groups exploited urban terrain and created ambushes, created a conventional arsenal using light artillery and other explosive devices. These hybrid and undetectable movements paralysed the country's economy since over a million civilians were temporarily evacuated, which had an ultimate psychological effect.

The Islamic State of Iraq and the Levant's military operations

The Islamic State in Iraq and the Levant (ISIL) has been carrying out military campaigns in Iraq and Syria since 2013 that show many characteristics of the concepts of hybrid warfare.

The proclaimed terrorist organization, founded in 2000, was said to be adopting, among others, actions such as bombings and artillery attacks, suicide and chemical attacks and aerial reconnaissance. Although those activities lie under conventional military offensives, ISIL involves a network of local supporters and informants that leak governmental information and meanwhile promotes information disorder through the use of propaganda.

Fields Affected By Hybrid Threats

In order to mitigate the impact of and finally tackle the issues surrounding the field of hybrid threats and asymmetric warfare, it is vital to fully comprehend and distinguish the different fields that those new offensives engage in to realise which measures should be developed. It is also of huge importance to understand why these phenomena pose a threat to the national and, of course, international security and compare such with the conventional (military) methods to establish a spherical perspective upon them.

¹Marcin Andrzej Piotrowski, "Hezbollah: The Model of a Hybrid Threat," PISM Bulletin, no. 24, March 2015

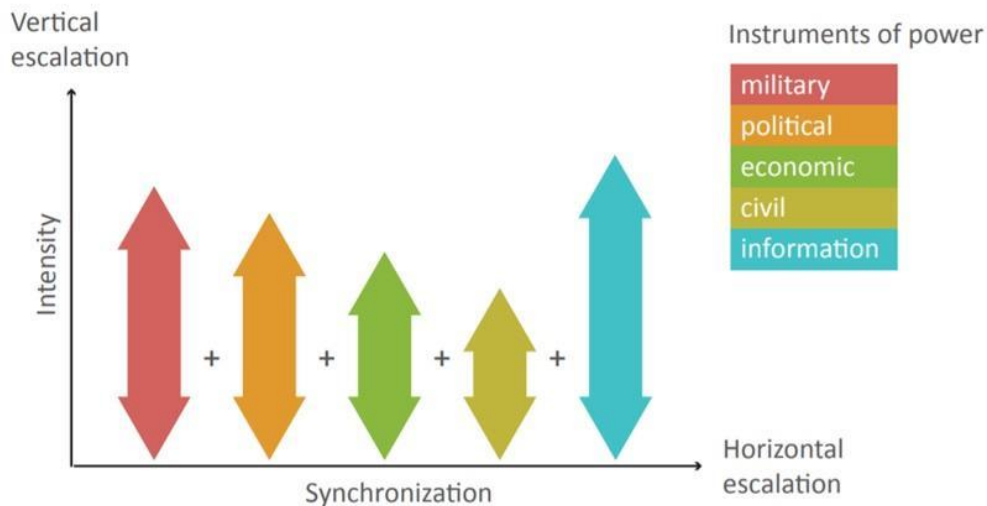


Figure 1 depicts a graph, which shows the fields affected by hybrid warfare²

It is widely known that hybrid threats synchronize the use of different instruments of governmental power that target different vulnerabilities across the contrasting societal functions of a state. Although hybrid threats branch out to a wide variety of fields, that does not necessarily mean that a hybrid threat should target all of such simultaneously. The functions that are disrupted are among others the economy, military and political information. Nevertheless, there are multiple cases where it has been noted that only certain individuals were impacted by carrying out similar activities.

Hybrid Threats in the Financial Sector

It is a fact that no specific scientific projects have been published that target the issue of the impact that hybrid threats have on the financial sector of society. Nevertheless, it is worth mentioning that the aim of hybrid threats is to employ a certain strategy so as to achieve a set goal without exceeding the threshold and causing a war.

Economic warfare is considered an important component of hybrid activities and it is to be seen at its highest in regions of corruption, cronyism, poverty and bad governance. One characteristic example of economic warfare is Pakistani's politico-economic background since all of the aforementioned phenomena are present in the area.

²"Hybrid Warfare." Graph. www.emmanuel.eu/wp-content/uploads/2018/06/escaleren.jpg.

This type of hybrid warfare targets the political field of a nation as well as the military sector of a country. Through the use of economic means that vary from tariffs or sanctions to a complete economic embargo, a party can, among others, entirely damage a country's trade industry, thus causing a huge financial crisis in the affected areas.

Hybrid Threats in the Military Sector

The impact that hybrid and asymmetric warfare have on the military is more than clear. Hybrid attacks do not necessarily involve the entailment of conventional weapons or military equipment, but there are cases, where unique military strategies are adopted. Such strategies mainly focus on the establishment of the element of psychological burden, which also has a relative connection with the element of surprise.

All the above are to be recognized in the Israeli-Hezbollah dispute which engaged in the development of unconventional military strategies that led to the escalation of economic issues and a generally negative impact on different fields of society.

Of course, it should not be misunderstood that hybrid attacks do not occur as conventional military methods. In fact, hybrid attacks simultaneously adopt both conventional and unconventional military ways, thus conventional military strategies and equipment can also be used in certain cases.

Nevertheless, hybrid threats only sometimes lead to the escalation of a military dispute, bearing in mind that their main goal is to remain undetected and target other societal factors (i.e. economy) and not just the military field.

Hybrid Threats and Propaganda

Information has a huge impact on society. It is crucial for decision making, political practices, diplomatic relations and it greatly influences public opinion. Thus, manipulating information could potentially be a great strategy that could lead to damaging a nation's reputation and integrity.

Hybrid warfare strategies are, as previously stated, highly connected with psychological operations by combining such with communication strategies. Managing a country's communication, promoting propaganda and appropriately controlling the mass media would lead to shaping the public opinion in a way that would be more devastating than any financial or political crisis.

In the globalized society, propaganda has been easier to implement. An individual, organization or country has an immense number of different ways to manipulate the public, whether those ways could be achieved through organizing false campaigns or by leaking false information about a group in social media.

Hybrid Threats and Civilians

One of the key characteristics that hybrid threats share is the fact that this type of warfare can indirectly involve civilians and ensure civilian control in order to achieve a major goal.

For the past 20 years, hybrid actions involving civilians have drastically increased. Organizations as well as governments have been manipulating the public through propaganda and misinformation, which are both carried out through the launch of campaigns.

This type of hybrid threat has many similarities with the engagement of propaganda in hybrid warfare. One could also argue that these two types could be aiming at the same objectives since both are based on the phenomena of misinformation and manipulation of the public. Nevertheless, there are slight differences between such.

Although both rely on the misinformation of the public, the engagement of hybrid threats in civilians could be targeting the assassination of important figures so as to cause mayhem and chaos in the society. Such operations have been held in the past, where important political figures were assassinated to prevent the escalation of upcoming issues and establish an environment of fear and stress.

Significance of Hybrid & Asymmetric Warfare

In order to effectively limit the use of hybrid and asymmetric warfare, it is vital to fully comprehend and distinguish why those phenomena are posing a huge threat to the international security environment.

Significance of Hybrid Warfare

As previously elaborated upon in the study guide, hybrid warfare synchronizes different instruments that all constitute government power and, by using such, it manages to achieve goals that conventional warfare would never be able to attain. Hence, managing to reach certain goals without necessarily engaging in military actions is one of the greatest points that hybrid warfare can have.

Furthermore, another point that conventional warfare could never manage to carry out is the fact that a great number of hybrid operations held have successfully remained secret for a long time before being detected by governments or organizations. This fact ensures that the respective hybrid operation will not be delayed or postponed due to the development of certain implications with governmental forces.

Significance of Asymmetric Warfare

As proven true throughout human history, conventional armies and conventional military strategies have a tendency of not being successful compared to more innovative ones. Armies with different sizes and different weaponry are always observed to be fighting using different ways and methods.

Traditional military strategies and tactics can nowadays be proven impractical, taking into consideration that such are worldwide known and adopted by almost every country or group. The significance of asymmetric warfare is based on the fact that through guerilla tactics the enemy is intended to be harassed and not completely eliminated.

The aforementioned fact is what differentiates conventional military practices from asymmetric warfare. Damaging an army's infrastructure, carrying out small raid operations and invasions, which are held during unexpected times, are some of the tactics that are followed in asymmetric warfare.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

North Atlantic Treaty Organization (NATO)

NATO is the main organization that has taken measures to tackle the issues of hybrid warfare and limit their impact, bearing in mind that such are posing a huge threat to international security.

Since 2015, NATO has developed a strategy, whose role is to counter possible hybrid threats that could negatively affect the alliance. NATO is currently attempting to detect any possible hybrid activities in order to prevent such as soon as possible. Supporting the allies' efforts to limit the extent of possible threats, NATO has accumulated a group of experts on the issue, which provides nations with the necessary civil preparedness and further information upon the aforementioned threats. Additionally, NATO has made further efforts

(i.e. to provide advanced technological equipment) to strengthen each government's security so as to limit any possibility of a hybrid operation taking place in the concerned areas.

European Union (EU) & Council of Europe

The European Union as well as the Council of Europe is a further alliance that has taken a stand against the hybrid international security threats. Exactly as NATO has done, the EU has more thoroughly investigated the possibility of currently having a hybrid operation being carried out, while the Council of Europe has released a large number of resolutions aiming to combat this issue.

Furthermore, the EU is trying to adopt a list of measures so as to reduce the possibility of a hybrid threat outbreak. Such are, among others, attempting to change the post-cold war geopolitical environment and developing new legal documents without vulnerabilities inherent in the phenomenon of globalization and the global market.

Concerning the documents that the Council of Europe has released, it should be mentioned that in 2017 the Council drafted the "Cyber Diplomacy Toolbox", which focused on the issues of cybersecurity and tried to eliminate the EU's "cybersecurity loopholes".

EU organizations such as the European Union Agency for Law Enforcement Cooperation (EUROPOL) and the European Union Agency for Cybersecurity (ENISA) have also engaged in those issues and have tried to improve the EU's technological environment to ensure a better outcome.

Russian Federation

While hybrid warfare is not as common of a practice as for the United States of America or any other western democratic state, the Russian Federation is one of the most known countries to be carrying out hybrid operations since the outbreak of the cold war.

The Russian Federation has multiple times adopted hybrid activities which vary from the Russian invasion in Georgia (2008) to the Russian actions in Crimea (2014). Throughout its hybrid war history, the Russian Federation has carried out a few hybrid operations against its past adversaries, which include organized agencies funded by the state, which always have had the role of being the undertaker of active interventions. Recruiting specific organizations such as Information Operation Groups, whose main goals are to carry out cyber information

activities and cause information disorder, exactly as done in the situation of Crimea, are to be seen in the aforementioned incidents.

China

China is a further state that has engaged in the fields of hybrid and asymmetric warfare, thanks to its stable historical background, bearing in mind that China's propaganda attempts to manipulate the public and its previous unique ways of handling the military have had a profound effect on the international community.

As far as asymmetric warfare is concerned, China has managed to develop new technological military strategies, thanks to the People's Liberation Army Navy (PLAN), which have been used multiple times and have been used in several operations throughout the South China Sea. China has also been involving civilians in its asymmetric attacks, especially those that are disguised as fishermen, who attack ships through the release of mines and artillery without being detected.

Sweden

Sweden is one of the main nations that have made significant initiatives to completely comprehend the origins of asymmetric and hybrid warfare. The Swedish government has organized campaigns and scientific projects to elaborate on any possible extent (i.e. economic, political, cyber) that such may have, bearing in mind that the European community has drawn a lot of its information about those phenomena from reports and articles drafted by Sweden. It is a prominent characteristic of all the documents created that Sweden criticizes and lists the actions of a variety of states that have engaged in those offensives and have finally resulted in the creation of chaos in the respective regions.

TIMELINE OF EVENTS

Date	Description of Event
2000	The founding of ISIL , which is one of the main terrorist organizations that has adopted asymmetric warfare strategies.
2006	The Israeli-Hezbollah dispute is the most modern example where hybrid actions were detected.
2008	The Russian invasion in Georgia is a further known example of the use of hybrid warfare, which firstly shows the Russian involvement in the issue.
2013	The ISIL's military campaigns in Iraq and Syria have stigmatised the international security environment since those were the first asymmetric military attacks adopted by terrorist organizations.

2015	NATO's project on tackling hybrid wars is the main project being carried out at the moment and it has provided the international security community with significant information about the issue.
2014	Russia's military actions in Crimea are also known as hybrid attacks, whose escalation was considered dramatic.
2017	The Establishment of "Cyber Diplomacy Toolbox" is a measure adopted by the EU, which focuses on the field of cybersecurity and ensures that the existence of hybrid activities in such will not take place.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

Security Council resolution 1935 (2010)³

This Security Council Resolution focuses on the issue of the hybrid operation in Darfur and condemns every attack claiming that every military operation is unacceptable. It proposes measures to combat it as soon as possible.

Declaration on Measures to Eliminate International Terrorism, 9 December 1994 (A/RES/49/60)⁴

This declaration deals with the issue of eliminating terrorism and bearing in mind that asymmetric warfare is a strategy, which is currently adopted by the ISIL and ISIS, this declaration is crucial. The aforementioned declaration adopts measures of tackling the issue of international terrorism and especially the organizations that adopt the tactics of asymmetric warfare.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

In the past there have been a few attempts made to tackle the issue of hybrid threats and asymmetric warfare both by the United Nations and other organizations. As far as the UN is concerned, both the Security Council as well as the General Assembly have adopted some resolutions concerning certain military disputes and whether those are based on hybrid or

³UN Security Council, *Security Council resolution 1935 (2010) [on the extension of the mandate of the African Union-United Nations Hybrid Operation in Darfur (UNAMID)]*, 30 July 2010, S/RES/1935(2010), available at: <https://www.refworld.org/docid/4d270ff72.html>

⁴UN General Assembly, *Measures to Eliminate International Terrorism - Report of the Secretary-General*, 6 September 1996, A/51/336, available at: <https://www.refworld.org/docid/3ae6b3250.html>

asymmetric strategies. Thus, it is clear that the UN has not specifically targeted the issue as a whole. NATO has released a large number of reports and articles concerning the aforementioned issue and has developed some ways to limit the impact of such in its allied countries. Last but not least, the Council of Europe seems to be the only alliance to have released resolutions specifically targeting the issues of hybrid wars and asymmetric warfare.⁵

POSSIBLE SOLUTIONS

Strengthening each sector of society

Through the development of every affected sector of society, it would become even more difficult for other parties, nations or organizations to carry out hybrid activities, taking into consideration that every sector that is influenced by hybrid warfare will be strictly regulated and thus even harder to manipulate. Each sector should develop different measures in order to prohibit this phenomenon (i.e. hybrid threats and propaganda could be tackled by stricter censorship of false information online).

Creation of legal background

It is vital to develop legal documents (i.e. conventions) upon this issue, so as to set a legal basis that every nation should follow, in order to firstly limit the existence of such threats nationally, and secondly to set boundaries that nations should abide by in their international diplomatic relations.

The imposition of penalties and punishments

It would be effective to urge the Security Council to impose penalties and sanctions on states or organizations (i.e. exclusion from international events, the imposition of financial sanctions) that do not follow the already existing legal frameworks upon this issue and constantly put the sake of the international security community in danger by repeatedly carrying out extravagant hybrid or asymmetric activities against other countries. Those penalties will be based on the accusation of violating international law.

⁵"Parliamentary Assembly." *PACE - Resolution 2217 (2018) - Legal Challenges Related to Hybrid War and Human Rights Obligations*, 2018, <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24762>.

Creation of a guideline for the use of hybrid and asymmetric attacks

The international community should decide and set specific situations, where those phenomena could be implemented, taking into consideration that these are considered extremely effective in solving disputes or deescalating already existing ones. It should also decide to what extent those strategies should be followed, in order for such not to be posing a huge threat to the international community.

BIBLIOGRAPHY

Bachmann, Sascha D. "HYBRID WARS: THE 21st-CENTURY'S NEW THREATS TO GLOBAL PEACE AND SECURITY."

ung.edu/institute-leadership-strategic-studies/uploads/files/bachmann-gunneriusson-hybrid-wars-16-sep-2016-scientia-militaria.pdf?t=1569110400096

Bennett, Bruce W. *RESPONDING TO ASYMMETRIC THREATS*. RAND Corporation, www.jstor.com/stable/10.7249/mr1576rc.11.

Carter, Ashton B. "Countering Asymmetric Threats." www.belfercenter.org/sites/default/files/legacy/files/chapter_5.pdf.

Gilles, Keir. "'Hybrid Threats': What Can We Learn From Russia?" *Bundesakademie Für Sicherheitspolitik*, 13 Sept. 2019, www.baks.bund.de/en/working-papers/2019/hybrid-threats-what-can-we-learn-from-russia

Gjørøv, Gunhild H. "Hybrid Warfare and the Role Civilians Play." *E-International Relations*, 8 June 2020, www.e-ir.info/2018/08/02/hybrid-warfare-and-the-role-civilians-play/.

Gressel, Gustav. "Protecting Europe Against Hybrid Threats." *ECFR.EU*, 25 June 2019, www.ecfr.eu/publications/summary/protecting_europe_against_hybrid_threats.

Long, David E. "Countering Asymmetrical Warfare in the 21st Century: A Grand Strategic Vision." *Center for Contemporary Conflict*,

MCDC. "MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare." Jan. 2017,

www.assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Miracola, Sergio. "Chinese Hybrid Warfare." *ISPI*, 21 Dec. 2018, www.ispionline.it/en/publicazione/chinese-hybrid-warfare-21853.

Mitrovic, Miroslav. "GENESIS OF PROPAGANDA AS A STRATEGIC MEANS OF HYBRID WARFARE CONCEPT." www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2018-1/70-2018-1-05-Mitrovic.pdf.

NATO. "NATO's Response to Hybrid Threats." *NATO*, 5 May 2020, www.nato.int/cps/en/natohq/topics_156338.htm.

Shambaugh, George. "Economic Warfare." *Encyclopedia Britannica*, www.britannica.com/topic/economic-warfare.

Wither, James K. *Making Sense of Hybrid Warfare*. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, www.jstor.org/stable/10.2307/26326441.