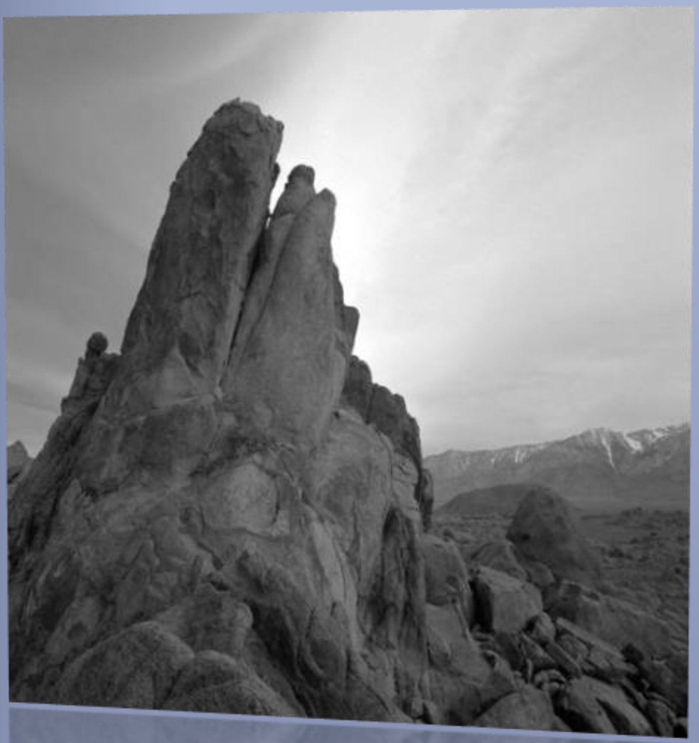

Hybrid Warfare: Theory, Case studies and Countermeasures

Κυριάκος Ι. Ιωάννου(ΑΜ: ΜΘ21019)

Διπλωματική Εργασία για το ΠΜΣ ΔΕΣ Πανεπιστημίου Πειραιά

Ακαδημαϊκό Έτος 2021-2022

Επιβλέπων καθηγητής: Επίκουρος Καθηγητής Δρ. Ιωάννης Κωνσταντόπουλος.

Μέλη τριμελούς επιτροπής:

Καθηγητής Δρ. Αθανάσιος Πλατιάς

Καθηγητής Δρ. Κωνσταντίνος Κολιόπουλος

Επίκουρος Καθηγητής Δρ. Ιωάννης Κωνσταντόπουλος

Το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία είναι αποκλειστικά ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται έχουν αντληθεί από άλλες πηγές, έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον τελώ εν γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου αφαιρείται ανά πάσα στιγμή αμέσως ο τίτλος. / The intellectual work fulfilled and submitted based on the delivered master thesis is exclusive property of mine personally. Appropriate credit has been given in this diploma thesis regarding any information and material included in it that have been derived from other sources. I am also fully aware that any misrepresentation in connection with this declaration may at any time result in immediate revocation of the degree title.

ACKNOWLEDGEMENTS

I would like to thank Dr. Ioannis Konstantopoulos, Assistant Professor of the University of Piraeus, for his remarkable help and contribution during the writing of this dissertation and for his assistance in answering every single question I had about this project. In addition to this, I would like to thank Dr. Athanasios Platias and Dr. Konstantinos Koliopoulos for their contribution to the bibliography of this review project, and also all the Professors of the University of Piraeus with who I cooperated during the courses, for accepting me in the MA of International and European Studies Programme and helping me in order to gain valuable knowledge and experience even though my difficult profession schedule. Last, nothing would have been fulfilled without the love, support and patience of my family. I thank and love them from the bottom of my heart.

Kyriakos I. Ioannou,
7th of September 2022.

To my family at whom
I own everything.

CONTENTS

ABSTRACT

During the last two decades, many conflicts have been declared all over the world and in many forms, using several kinds of weapons. All of these have caused the transformation of the conventional ways of fighting in a more mixed procedure, leading us to refer to them by using the term **Hybrid Warfare (HW)**. In this qualitative review dissertation, has been made a theoretical approach to the definitions of the HW and the characteristics of the numerous Hybrid threats. Additionally, the reference to historic paradigms and case studies from the past and present, underlines the fact that the tactics of the HW can be executed by both state and non-state actors, posing additionally a great pressure in the change of the strategic doctrine of many militarily and politically powerful countries, such as USA and Israel. On the other hand, it is very useful the examination of the countermeasures against the Hybrid threats implemented by organizations such as the NATO and the EU, which actually put together systematically the adding force of their member-states. Finally, the concluding remarks emphasize on the lessons learned by the up to nowadays analysis of this phenomenon.

Key Words: Hybrid Warfare, Hybrid Threats, Four Block Wars, Gerasimov’s doctrine, Second Lebanese War, EU Hybrid Fusion Cell, NATO’s Allied Command Transformation (ACT).

Περίληψη

Τις δύο τελευταίες δεκαετίες, έχουν ξεσπάσει πολλές πολεμικές συγκρούσεις ανά την υφήλιο, οι οποίες έχουν λάβει διάφορες μορφές σε σχέση με αυτές του παρελθόντος, χρησιμοποιώντας μάλιστα νέες τακτικές, μεθόδους και όπλα. Όλα τα ανωτέρω έχουν οδηγήσει στην «μετατροπή» των συμβατικών μεθόδων διεξαγωγής πολέμου σε μία νέα πραγματικότητα. η οποία συνδυάζει παλαιές και πιο σύγχρονες (μη συμβατικές) στρατηγικές, αναγκάζοντάς μας να αναφερόμαστε σε αυτές με τον όρο **Υβριδικός Πόλεμος**. Στην παρούσα βιβλιογραφική έρευνα εκτελέστηκε μία θεωρητική προσέγγιση στην περιγραφή των ορισμών του Υβριδικού Πολέμου, αλλά και στην παράθεση των χαρακτηριστικών των αναρίθμητων Υβριδικών Απειλών. Επιπρόσθετα, η αναφορά σε ιστορικά παραδείγματα αλλά και γεγονότα από το παρελθόν μέχρι σήμερα, υπογραμμίζουν το γεγονός ότι οι τακτικές του Υβριδικού Πολέμου μπορούν να χρησιμοποιηθούν από κρατικούς και μη δρώντες, επιβάλλοντας μία επιπρόσθετη πίεση στα πολιτικοστρατιωτικά επιτελεία πολλών μεγάλων δυνάμεων, όπως οι ΗΠΑ και το Ισραήλ, αναφορικά με την αλλαγή του στρατηγικού τους δόγματος. Παράλληλα, είναι πολύ χρήσιμη η μελέτη των αντιμέτρων κατά των Υβριδικών Απειλών που εφαρμόζονται από οργανισμούς όπως το ΝΑΤΟ και η ΕΕ, οι οποίοι κατ' ουσίαν αθροίζουν συστηματικά την δύναμη των κρατών-μελών τους κάτω από την οργανωσιακή «ομπρέλα» τους αναφορικά με το εν λόγω κίνδυνο. Καταλήγοντας, γίνεται μία επιπρόσθετη αναφορά στα συμπεράσματα που έχουν εξαχθεί διεθνώς από την έως τώρα ανάλυση των περιπτώσεων Υβριδικών Συγκρούσεων.

Λέξεις Κλειδιά: Υβριδικός Πόλεμος, Υβριδικές Απειλές, Πόλεμος Τεσσάρων Περιοχών, Δόγμα Γερασίμοφ, Δεύτερος Πόλεμος Λιβάνου, Κέντρο Διάχυσης Υβριδικών Απειλών ΕΕ, Μετατροπή Διασυμμαχικής Διοικητικής Δομής ΝΑΤΟ.

CHAPTER 1

Introduction

The present review MA dissertation describes the phenomenon of Hybrid Warfare, which is the nowadays biggest and state-of the-art threat of the Western Democratic States, the characteristics of the Hybrid Threats, mainly by the description of two Hybrid Warfare case studies, and the countermeasures against this type of conflict that have been taken by the two strongest worldwide civil-military organizations: NATO and EU.

The strong necessity by which the study of this type of warfare is derived is the high rate in which it appears worldwide, both by state and non-state actors during peacetime, crisis and war periods. Obviously, Hybrid Threats can be used as a "tool" of diplomacy and mean of political pressure and at the same time as an "ally" of terrorist organizations. Another useful remark is the vast variety of ways and methods that can be implemented, from cyber attacks, disinformation and fake news to trafficking and weaponizing of migrant crisis. All of these pose a complicated problem which needs a 24/7 early warning alert by the security agencies of both civilian and military structures.

There are many occasions in mankind's History whereas Hybrid Warfare appeared as it will be described thoroughly in the first chapter. However, the severe breakthrough was done after the 9/11 terrorist attack against USA which alerted the whole Western Security system, followed by the wars in Afghanistan (2001) and Iraq (2003) which in turn caused the change of strategic doctrines in general. At the same time, the Second Lebanese War (2006) and the Russia-Ukraine conflict in Crimea (2014) enlighted many aspects and features of the modern hybrid conflicts.

It is of high importance the theoretical analysis and studies of Frank G. Hoffman and James N. Mattis. Both of them, as retired officers of US Army, worked on the formulation of the modern US strategic doctrine by setting as main threat the hybrid one and by analyzing its different shapes that can have in every single type of operational environment (land, marine, air, civilian). By that way, it is easier to propose measures against them.

As this study shows and in my opinion, the way of countering hybrid threats starts from the society and especially during the first years of our lives, inside the family and school environment. It has to do with the ability of critical thinking that students grow, on the way they will study and learn to live among multicultural democratic free-thinking states. By creating such kind of societies, many categories of hybrid threats that have to do with cultural and religious extremism will be diminished. However, as our world is in a constant war between good and evil, on the strategic and tactical level, it is proved that Western Democratic States have to unify their efforts in order to face this kind of adversaries, mainly in the structural context of worldwide civil-military organizations, such as NATO and EU.

So, in this bibliographical dissertation the posed questions on what hybrid challenges are and how could be faced, will be answered by the analysis done in the following four axes:

- Conventional and Non-Conventional methods and tactics.
- Theoretical approach.
- Historic and recent case studies.
- Countermeasures.

The first chapter consists of an in depth analysis of the concept and the basic characteristics of the Hybrid Warfare. In the second chapter, there is the description of a hybrid warfare among state actors such as Russia and Ukraine, while in the third chapter is posed the example of the second war in Lebanon, which is a typical paradigm of non-state actors Hybrid Conflict. During the fourth chapter are proposed the measures that states and non states have to take in order to face hybrid opponents and accordingly the actions that have so far been taken by EU and NATO. Finally, in the last chapter there concluding remarks of the whole analysis are presented.

CHAPTER 2

Concept of Hybrid Warfare

2.1 Introduction

"War is the father of everything" Greek philosopher Heraclitus said 2,500 years ago and seems that his "obscure" quote survived until nowadays and proved, more or less, to be true. Due to the fact that, especially under the point of view of the realist theory, the states, which are the main actors of the anarchist International system, will try first of all to survive and then to keep (if not to expand) the relative power they have in the world (Platias, 1995, 2012, 2020 ; Waltz, 2011).

As the "three great minds" of Strategic Theory –Thucydides, Sun Tzu and Carl Philipp Gottfried von Clausewitz- have stated in their monumental works (and in their own way, having of course differences in their theories), war, and in general military operations, is a political action and both political and military leaders are in continuous cooperation for the achievement of the state's aims. But also during the peacetime, a country has to be well prepared and have the necessary economic, technological and military resources by itself in order to be able to face successfully every single enemy whenever will be necessary to (Thucydides, 1940 ; Platias & Koliopoulos, 2015 ; Clausewitz, 2007).

2.2 Defining the Hybrid threat-Methodology of the Dissertation

Maybe the most demanding step in the continuous process of the Command Control Communications Computers Intelligence Surveillance Reconnaissance (C4ISR) in a state is the definition and clarification of the upcoming threat, both in peacetime, period of crisis and wartime. In order to have such a robust and continuously operating and information producing cycle, military and political leaders will have to bear in mind that an inner (but very important) cycle has to be working non-stop and efficiently: **John Boyd's Observe Orient Decide Act (OODA) Loop (Figure 1)** (Koliopoulos, 2008, p. 245-247). This easily memorable Rule Of Thumb (ROT) helps commanders taking decisions and acting quickly, having at the same time a feedback mechanism which will near-automatically (according to its inner design) correct any observable mistake or near-miss.

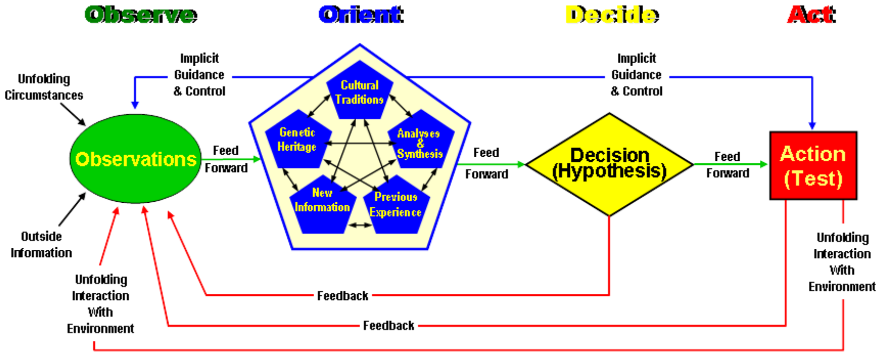

Figure 1: John Boyd's OODA Loop

Source: https://www.foresightguide.com/boyd-competitive-dominance-cycle/

A very important stage of the abovementioned cycle is the information that gets transferred from each and every level of command. This kind of information (Konstantopoulos, 2010, p. 37-56) gets numerous forms depending on the transmitter (originator of the information), the channel in which the information flows and its specific form. From these aspects, the best way to describe the term "information" (intelligence, data, e.t.c.) is through the following "pyramid" (Figure 2):

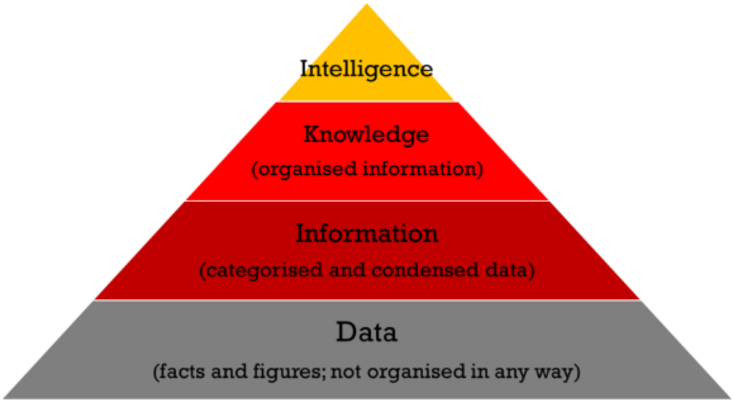
Intelligence
Knowledge
(organised information)
Information
(categorised and condensed data)
Data
(facts and figures; not organised in any way)

Figure 2: The Data-Information-Knowledge-Intelligence (DIKI) pyramid

Source:*https://ec.europa.eu/research/participants/documents/downloadPublic/eVR5Sjg1ZE5xaFhSUDltS0x2ZXlWK2JBYnRoaEo5ejVHcGtOTkNCU2p5Y1F1b3ZORk5MYkh3PT0=/attachment/VFEyQTQ4M3ptUWVUNDZMNjBqS2NMQkhTSjA1WWFORkM*

As it was stated in the introduction of this dissertation, the hybrid threats are the state of the art in the modern warfare. However, it is not a new term. In this chapter, actually, it will be emphasized that it is synchronous with the history of war. During the Trojan War, Ulysses was one of the first innovators of the hybrid tactics by using the Trojan Horse (art of deception). In addition to this, as Thucydides informs us (Platias & Koliopoulos, 2010 ; Mansoor, 2012, p. 3-4), during the first years of the Peloponnesian War, Spartans, apart from the external enemy –the Athenians- had also to face their inner enemy, the slaves *Helots*. The majority of them where situated in Laconia and Messenia (Figure 3) and so Spartans had to keep numerous soldiers in these regions in order to prevent an uprising of them, who were also very important backs for their agricultural and military systems. As Williamson Murray and Peter R. Mansoor state, Athenians wanted to build a base at Pylos (which is situated on the southwest coast of the Peloponnese) in 425 BC in order to assist Helots to rise against Spartans. Outside of this fortress, Messenians from Naupactus, whose ancestors were expelled by the Spartans since 464 BC, were situated and started coming into contact with the Helots of Laconia, helping them to fight against Sparta and thus becoming an ally of Athens. Of course, the whole strategic move was an exceptional hybrid tactic. (Platias & Koliopoulos, 2010 ; Platias & Trigkas, 2021)

As a side note, this strategy of the Athenian leader Pericles is a strong argument that the Thucydides' Trap was just a misunderstanding (especially in the translation of the ancient text) and the Peloponnesian War was a war of choice and not an inadvertent escalation between Athens and Sparta (Platias & Trigkas, 2021).

Figure 3: Spartans being attacked in the battle of Sphacteria. Artwork by Peter Dennis (Source: Wikimedia Commons)

Source: https://historyofyesterday.com/the-only-time-the-spartans-ever-surrendered-30a191441bee

Also, Sun Tzu through his indirect approach on warfare was one of the first theorists of the hybrid tactics, as he would insist that the biggest win of a leader is to defeat his enemy by winning him without a battle, by only causing him damages in his economy, through intelligence and driving him into considerations on whether he would gain enough for the risk he would take in such a war (Platias & Koliopoulos, 2015). On the other side, Clausewitz was supporting the tactic of the direct approach on war through the destruction of the enemy's army, who was, in his opinion, the main Center of Gravity (CoG), as the part of intelligence (which of course is important and is one of the main characteristics of the hybrid threats) remains under the *"fog of war"* (Clausewitz, 2007).

In addition to him, Niccolo Machiavelli faced also in his own city, Florence, an aspect of hybrid threat, the mercenaries, who could at any time become from allies enemies as their only homeland is money (Gilbert, 1986). Another famous paradigm is that of T. E. Lawrence, also known as *"Lawrence of the Arabia"* (Figure 4), who played a significant role during the Arab Revolt (1916-1918) against the Ottoman Empire during the First World War.

Figure 4: Lawrence of the Arabia

Source: *https://www.nytimes.com/2010/11/22/books/22book.html*.

"Building" the definition of hybrid warfare and hybrid threats firstly we can point out that they coexist with the conventional warfare. Actually, they are the sum of conventional and unconventional strategies as a whole, which will be explained further on this dissertation, and on a parallel line it is the mixed combination of all the types of warfare together (Mattis & Hoffman, 2005, p. 1-2).

In the modern era, the Revolutions in Military Affairs (RMA) began from the USA during the dawn of the 21st century and more specifically after their warfare experience in Afghanistan (2002) and Iraq (2003). Furthermore, as it is already known, USA is the main and strongest country in the world in terms of military power, technology and industry. However, in the abovementioned wars, USA faced severe difficulties and casualties in the urban warfare operational theater due to the asymmetric tactics of their opponents who also had the advantage of the environmental awareness as they were natives. So, these facts convinced the USA Armed Forces Headquarters (and especially the former Minister of Defense of the Trump's administration- then Lieutenant General- James N. Mattis) that the RMA had to be based not only in technology but on similar terms on the human dimension in warfare. Social, political, and technological forces can also change the characteristics of armed conflicts, but they cannot change its fundamental nature, which is the human behavior under threat. This fact was followed by the completion by the Pentagon of its Quadrennial Defense Review (QDR) whereas was made clear that in order for the US Forces to maintain their worldwide superiority they had to pass from **dominance** to **revelance**. In the first domain, as it was said before, US have no opponents. However, revelance is a more complicated term, as it is the decision on where and how a force is going to attack its enemy in dependence of where this threat is getting concentrated to fight. So, the strategic priorities in the QDR got renewed and the US forces got trained to combat in the *"contested zones"* of urban and other complex terrain in order to not experience again the great numbers of casualties they had in Afghanistan and Iraq (Mattis & Hoffman, 2005, p. 1-2).

Accordingly, the new National Defense Strategy (NDS) of USA lays out four emerging threats; the traditional, the irregular, the catastrophic, and the disruptive. While state-based conventional threats still exist, it is with no doubt that the United States will dominate this kind of adversaries in the foreseeable future. This superiority creates a compelling logic for states and non-state actors to move out of the traditional mode of war and seek some unexpected combination of technologies and tactics to gain sort of advantage and balance the situation. This fact is translated into the rise of irregular challengers who seek to exploit tactical advantages at a time and place of their own choosing, rather than complying to "the conventional rules" of war. They accumulate a series of small tactical effects magnifying them through media and by applying Information Warfare (IW) tools. Consquently, future wars will have the form of "Four Block Wars": Fighting on one block, preserving humanitarian supplies to the civilians in the next block and at the same time keeping local warring factions apart. At the third block a force has to deal with the psychological or IW aspects, mainly by communicating or broadcasting the narration to the habitants of the area where the whole operations is being held (Mattis & Hoffman, 2005, p. 1-2).

Another dimension added is situations like the **counterinsurgency** in Iraq, which is the fourth block of the abovementioned scheme. Insurgencies are wars of ideas which need to compete and get superior against those of the enemy. Actions in the first three blocks are important in order to build up credibility and establish smooth relationships with the local population and their leadership. However, there is an Information Operations (IO) aspect within each block on how the armed force will influence those populations to reject the misshaped ideology and hate they have against the operating armed force (Mattis & Hoffman, 2005, p. 1-2).

According to Frank G. Hoffman (2010) hybrid threats are defined as any adversary that simultaneously employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battlespace to obtain their political objectives. In addition to, hybrid threats incorporate combinations of different modes of warfare including: conventional capabilities, irregular tactics and formations, terrorist acts mainly involving violence and coercion. These multi-modal operations display a vast variety of operational and tactical fusion in time and space. (Hoffman, 2010, p. 443-444).

Additionally, Peter R. Mansoor (2012) gives the features of HW and Hybrid Threats underlying the fact that hybrid opponents form a difficult and often powerful enemy, because as the existence of conventional forces requires a military force to mass against them, at the same time logistical lifelines and contested areas get vulnerable to insurgents, guerrillas and other irregular forces ready to act. Moreover, it has been examined that hybrid adversaries have been willing to extend wars in time and space to achieve their goals, because in the majority of the occasions, (if only great powers possess a deep commitment) time is on the side of the less powerful hybrid opponent. Therefore, when the clock runs out, the side that possesses the ground wins by default. This temporal aspect has represented a major challenge to militaries engaged in conflict outside their homelands against hybrid adversaries, a point made by T. E. Lawrence when he wrote of the Arab revolt: *“Final victory seemed certain, if the war lasted long enough for us to work it out.”* So, hybrid adversaries test the strategic patience of their opponents. Another aspect that has to be pointed out is that while conventional military forces conduct operations to defeat their regular opponents, other military forces and interagency assets must work to clear areas of irregular forces, to control those areas over the long term and to counterorganize the population in order to pacify it. Military success and the establishment of legitimacy among the population will lead to increased home-front and international support, without which great powers risk defeat as it was also stated by General Mattis in the Four Blocks War theory. Political leaders set national objectives, work to bolster national will, and build and keep intact international coalitions to share resource burdens and they must understand the nature of their opponent as well as the extent of the commitment necessary to win the war. At the same time, military leaders must adjust existing doctrine to take into account the kind of war in which their forces engage, as well as to counter enemy strengths and exploit enemy weaknesses. Senior leaders must create viable operational concepts that link strategy to tactical actions and leaders at all levels (political, strategic, operational, tactical) must gather lessons learned from ongoing military operations and alter doctrine, operational concepts and strategy to meet unexpected challenges and opportunities. In conclusion, leadership is the top priority (Mansoor, 2012, p. 4, 5, 7, 9, 10, 17).

This is why Ayodele A. Otaiku (2018) states that in order to form a national strategy (generally and especially against Hybrid Threats) it is of high importance to employ the decision maker's strategic thought upon the scheme Ends, Ways and Means as follows:

Policy ("How do we do it?" and "What do we do?")→**Strategy** (Strategic Doctrine and Grand Strategy)→**Operations** (Military Doctrine)→**Tactics** (Otaiku, 2018, p. 2).

Dr Andrew Mumford (2016) provides us another useful explanation of what HW is bearing in mind the terrorist aspect of these threats, as in his opinion, HW transcends the monocausal modes of conflict that have dominated recent strategic discourse, such as insurgency or piracy. Instead, it encompasses a complex set of relationships, dynamics and processes. HW then gets transformed to a multicausal mode of conflict that takes place in environments containing multiple types of threats in which states and non-state actors interact (both covertly and overtly) using a mixture of regular and irregular war-fighting tactics for the purposes of extending influence, interest and, in some cases, territory, both in the real and in cyber space (Mumford, 2016, p. 7).

Finally, Jan Joel Andersson and Thierry Tardy (2015) refer to definitions about HW given by different nations and organizations, as this term first appeared in 2002 in a thesis written by William J. Nemeth at the US Naval Postgraduate School *('Future War and*

Chechnya: a Case for Hybrid Warfare'). It is worth noticed that in the US, the term 'hybrid' did not appear in any of the three National Security Strategies of 2006, 2010 and 2015. The 2015 National Military Strategy refers to 'hybrid conflicts' that may consist of 'military forces assuming a non-state identity, as Russia did in the Crimea, or involve a Violent Extremist Organisation (VEO) fielding rudimentary combined arms capabilities, as ISIL has demonstrated in Iraq and Syria, serving to increase ambiguity, complicate decision-making and slow down the coordination of the counterpart's effective responses (Andersson & Tardy, 2015, p. 2).

At this point, it is important to refer to the methodology that was followed in order to fulfill this project. As it was seen by the introduction and the abovementioned paragraph of this qualitative dissertation, the questions that were posed, examined and answered throughout the whole project are the following:

- What is Hybrid Warfare and which are the characteristics of the Hybrid threats?
- Is Hybrid Warfare a recent phenomenon or was created during the ancient years?
- Is Hybrid Warfare conducted by state and non-state actors?
- Which are the countermeasures proposed by worldwide organizations against the Hybrid threats?

The analysis that was held was based upon the research of bibliography consisted of books, articles, papers and reports from Greek and foreign scientists and officials. Information that was collected was cross checked among the references and was tested by the case studies and the historic paradigms that are presented. In that way, the concluding remarks in the last chapter concentrate the entire study that was done.

2.3 Characteristics of the Hybrid threat

Hybrid wars can be conducted by both states and non-state actors (as it will be described in chapters 3 and 4), by separate units or even by the same unit which operationally and tactically is directed and coordinated within the main battle space. Hybrid forces can effectively incorporate technologically advanced systems into their force structure and strategy and use these systems in ways that are beyond the intended manualdescribed parameters ('think out of the box' metho). In addition to this, they incorporate combinations of different modes of warfare including: conventional capabilities, irregular tactics and formations, terrorist acts and criminal disorder, confounding purely conventional approaches and kinetic solutions, foiling today's emphasis on population-centric counterinsurgency strategies (Hoffman, 2010) (Figure 5).

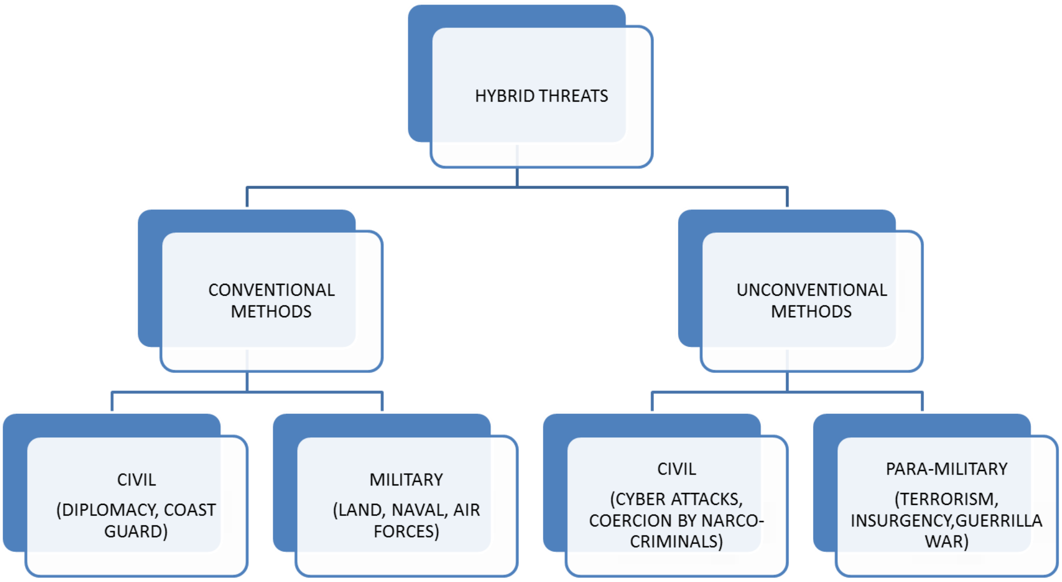

Figure 5: A typical diagram of Hybrid Threats (Hoffman, 2010)

The list of hybrid threats is synonym to infinity, as the fantasy of politicians and military leaders produces new methods. However, some of the most usual are the following:

- Cyber attacks against critical infrastructures and security systems of high importance.
- Influence upon the prices and distribution of natural resources.
- Support of demonstrations and strikes.
- Support of suspicious acts of Non-Governmental Organizations (NGO).
- Broadcasting news which try to influence individual's opinion upon certain issues and directions.
- Pressure upon policymakers and politicians having to do with the institution of laws.

- Support of national minorities.
- Action of paramilitary/guerrilla groups.
- Sabotage, blackmailing.
- Transfer of huge numbers of habitants under (violent) pressure.
- Control of critical economic functions.
- Water and food infection/contamination.
- Proxy wars (Konstantopoulos, 2020, p. 7, 12).

Every kind of warfare operations is consisted of certain phases in which events are seen as following a linear causal trajectory towards a specific end/target. Due to the fact that a HW campaign can operate along both the vertical and the horizontal escalation axes, it is unlikely that such a campaign will consistently follow a linear and causal trajectory where one stage always follows the other. Escalation will most likely be followed by periods of de-escalation, and vice-versa, to control the operational tempo. For instance, horizontal escalation of HW may occur in the form of battlefield preparations (like mapping adversary cyber networks, espionage) that may never escalate vertically and reach the "attack phase." Crucially, much of what is done in the horizontal axis might be ambiguous or not readily definable as a hostile and aggressive act, unless these resources are activated in a more explicit or intensified sense (Reichborn-Kjennerud & Cullen, 2016, p. 3 ; Richterová, 2015, p. 5-9).

Consequently, the HW phases are:

- **The preparation phase:** Enlights the steps, situations and decisions taken prior to the actual attack in order to secure advantageous environment to carry out the attack successively.
- **The attack phase:** The attack phase has to be the shortest of the three phases. It includes the chosen combination of available and known military and nonmilitary attack aspects, military, paramilitary and rebel units, terrorist and cyber threats.
- **Defending the end state phase:** It aims to ensure the sustainability and duration of the goals of the mission and usually includes series of political, diplomatic and military steps responding to current situation.

The above analysis shows how HW complicates the concept of phases in several ways for many reasons. First, it will be hard to discern a beginning or indeed an end to hostilities. Second, this blurring of distinctions leads to thinking about HW as a form of permanent war in which it is increasingly difficult to distinguish between normal legal activities, coercive diplomacy and war, resulting that HW is an unclear and unrealistic understood notion (Reichborn-Kjennerud & Cullen, 2016, p. 3 ; Richterová, 2015, p. 5-9).

2.4 Conclusion

All strategy is contingent. Successful strategy emerges as a product of the aims of the actor, the Strengths-Weaknesses-Opportunities-Threats (SWOT) analysis of their adversary, and the identity of the strategic environment. At the same time, as it was described above, there is needing of planning in detail each phase of warfare and taking into consideration its specific characteristics. Consequently, there are three key contextual factors that explain the rise of hybrid threats, specifically under the sight of the revisionist grand strategy used by state and non-state actors:

- The shifting balance of global and regional power, challenging the world status quo.
- Interdependence within the global political economic environment.
- Technological convergence (Monaghan, 2019, p. 85-87 ; Giegerich, 2016, p. 69-70).

Bearing in mind that both hybrid threats and HW describe distinct challenges to national security that are likely to endure and persist, the following conceptual distinction is therefore proposed:

- Hybrid threats combine a wide range of nonviolent means to target vulnerabilities across the whole domain of society to undermine the functioning, unity, while degrading and subverting the status quo.
- Hybrid warfare is the challenge presented by the increasing complexity of armed conflict, where adversaries may combine types of conventional and non conventional means to neutralize enemies' military power (Monaghan, 2019, p. 85-87 ; Giegerich, 2016, p. 69-70).

The implications of a hybrid approach to conflict are wide-ranging and cut across concepts, material capability aspects, legal matters, and institutional innovation.

Apart from the reasons that were stated above about how important is the study of the HW domain, two more historic events make it even more crucial:

1. The intelligence failure of US Forces during the Second Gulf War (2003), which showed that the inadequacy of preparation, the lack of essential information about the opponent’s warfare tactics and its environment and the rash of the policymakers in order to succeed their political goals can cost greatly in a nation-and so it drove them to change their NDS.

2. As it will be discussed in Chapter 4, during the second Lebanon-Israel war, the Israel Defense Forces (IDF) had to change their doctrine related to the urban warfare in order to face the Hezbollah troops (Fitzgerald & Lebow, 2006).

CHAPTER 3

State actors: Russia vs Ukraine case study

3.1 Introduction

As it was analyzed in Chapter 2, states are the primary actors of the HW due to the fact that they also are the main units of the International Political System. One of the basic factors and influencers of this system during the last 3 centuries is Russia (and its ancestor Soviet Union). As it will be described in this Chapter, Russia's war against Ukraine in 2014 is a unique and exceptional occasion of HW among two sovereign states and is studied under the domain of the revisionist policy of Vladimir Putin about the new "Great Russia".

3.2 Russia's revisionist policy-Gerasimov Doctrine

Russia had a significant role in the International System during the 20th century. However, it passed several times in different states of power and destruction, mainly after the collapse of the Soviet Union in 1990. Many political scientists, most of them influenced by the liberal school, believed that no wars especially of large-scale would ever been declared after the ending of Cold War. Unfortunately, they proved to be wrong. During the second decade of Vladimir Putin's presidency in Russia and after feeling that his country has to play a dominant role and be respectful by everybody in the International System, he wanted to resurrect the dream of the "Great Russia" and (up to 2022) to control and conquer the states which are situated near their borders (Belarus, Ukraine, e.t.c.) in order to get protected from the expansion of European Union (EU) and the North Atlantic Treatment Organization (NATO) eastwards in its "neighborhood". Therefore, Russia had to adapt a more aggressive strategy in every single domain (military, economic, scientific, social control, e.t.c.). The same happened with the HW strategy and doctrine (Kofman & Rojansky, 2015, p. 3-5).

Russian analysts use the terms “new generation warfare” or “non-linear war” when they refer to HW. The former was introduced to Western audiences through a paper published by General Valery Gerasimov, the Chief of the Russian General Staff, in February 2013. Consequently, the Russian approach to HW is known as the “Gerasimov Doctrine (Wither, 2016, p. 80).”

Gerasimov describes new generation warfare as the broad use of political, economic, informational, humanitarian and other non-military means along with civil disorder among the local population and concealed armed forces (Wither, 2016, p. 80). He also recognizes that many of these methods were not traditionally part of what would be considered wartime activities (as it was underlined in Chapter 2), believing that they are typical of 21st century warfare and actually more significant for the success of strategic goals than military means and so adapting an approach more relative to Sun Tzu’s indirect approach. Nevertheless, it is evident from Gerasimov’s paper that the armed forces have an essential supplementary role in new generation warfare. This is particularly the case with Special Operations Forces (SOF) that can be used under the disguise of peacekeeping and crisis regulation to link up with opposition groups inside a targeted state. The use of SOF under cover IO was clearly evident in Ukraine in 2014. Covert spetsnaz units (a.k.a. **“little green men”**) were employed to seize government buildings and key infrastructure targets and arm separatist militia, while the Russian government spread doubt and confusion through repeated denials of Russian involvement, except of the 17th of April 2015 when publicly was acknowledged that Russian SOF were involved in Crimea. Other techniques of hybrid or new generation warfare were used to demoralize and intimidate opponents. These included exercises by Russian conventional forces close to the Ukrainian border, cyber attacks on Ukrainian government systems and a wider diplomatic and media offensive to undermine the legitimacy of the new government of Ukraine. The ultimate aim of this sort of warfare is to apply pressure which will consequently cause the collapse of the target state from within so that the political objectives of the conflict can be achieved without any battle (Thiele, 2015a ; Wither, 2016, p. 81).

Many of the methods Russia has used in Ukraine date back to the Soviet era and the application of military deception also known as maskirovka, which was applied by Soviet forces during World War II and in Cold War proxy conflicts. In the 21st century, advances in information technology and processing have greatly increased the scope of maskirovka, allowing the Russian government to employ multimedia propaganda and misinformation on a large scale. These have been used to build support for the government's foreign policy within Russia and to wage a wider IW against Ukraine and the West. The concept of public's perception management is a key element of maskirovka. This originated with the work of former Soviet psychologist Vladimir Lefebvre who developed the theory while researching ways to influence and control an enemy's decision-making processes. The theory can be described as the use of specially prepared information that inclines an opponent to voluntarily make a decision that has been predetermined as desirable by the creator of the information. A wide range of actors, such as politicians, civilians and militias, conventional and non-conventional and their activities, must be coordinated and controlled to achieve the overall military and political objectives, taking into consideration their differing political interests (Wither, 2016, p. 82).

3.3 Timeline of the annexation of Crimea (2014)

The "soft power" of the EU and its ability to reshape the political and economic structures of post-communist states is a key challenge to Russia's security feeling. The Russian-Ukrainian crisis of 2014 occurred at this kind of intersection of geoeconomics and geopolitics EU intersts in the South West borders of Russian Federation (Wither, 2016).

When President Victor Yanukovich turned away from the EU in November 2013 and towards Russia the next month, receiving by the later a $15 billion loan and cheap energy supplies, a sharp public reaction was triggered leading to the occupation of Maidan Nezalezhnosti (Independence Square), thereby giving the revolution its name, 'Euromaidan'. Despite an attempt by the EU and Russia to reach an agreement between the government and the opposition, President Yanukovich fled to Russia on 24th of February 2014. Following this action, a transitional government was installed, which was condemned by Russia as illegal and extremist due to its threats of applying violence against the Russian population of Crimea. On 27th of February, Russian SOF combined with local activists took over government institutions in Crimea, as well as Sevastopol which is Russia's Black Sea Fleet harbour. Consequently, on 18th of March, these areas were annexed by Russia. In the following months, numerous deliberate measures were taken by Russia of course with local support, to destabilize Ukraine, mainly by taking control of government buildings in the most significant cities of eastern Ukraine. Meanwhile, a substantial military capability was maintained on the other side of the border, ready to invade. In addition, efforts were made to further destabilize an already unstable economy through export embargoes and threats to gas supplies and also threats to neighboring states, such as Moldova, Belarus and Kazakhstan, that could also be affected because of the Russian minorities in their territories (Wither, 2016).

The 2014 crisis represented a profound and possibly decisive official tilt away of Ukraine from the EU and towards Russia. There were fierce popular protests, which President Yanukovich handled unsuccessfully, firstly, with an attempt to introduce authoritarian measures, then seeking compromise, followed by shooting and, finally, a brokered deal on the 21st of February with the representatives of the EU and Russia. By this time, popular feeling was against the president and he left Ukraine, leaving behind evidence of startling and corruption-fuelled wealth. The transfer of power was irregular and improvised, and set precedents in terms of seizing buildings and setting up barricades as a means of coercing a government, while the parliament was still functioning. The new government was not ideal, but was better than could have been expected after the president's leave. Moscow's argument was that the US and the EU had played a significant role in the illegal overthrow of President Yanukovich, which was led by fascistic elements. However, details of what actually happened in Kiev from 20–24 February do not support these allegations. The most lethal and wrong act taken by the Ukrainian parliament after Yanukovich's flight was to vote that Ukrainian would be the sole state language at all levels. This caused a strong adverse reaction in Crimea and southern and eastern Ukraine, where the majority of habitants speak the Russian language and drove street protests. Acting President Oleksandr Turchynov vetoed the bill on 1 March. But actually, the real fear of Putin's administration was that a new government with a Western orientation posed a serious threat. Every action taken by Russia's side in the post-Yanukovich period has been geared to recovering this lost position, ensuring that Ukraine would be unable to join the EU by keeping it in a state of constant chaos and uncertainty. This has involved seeking to make it impossible for Kiev to organize the elections planned for 25 May 2014, coupled with demands for a more federal constitution that would have the effect of allowing the Russian-oriented eastern regions to block a close association with the EU. Additionally, it is less clear the fact whether the coercive diplomacy applied by Putin to undermine the new government in Kiev, by using SOF and local activists to establish a presence hostile to the central government have represented a form of pressure that could in principle be turned off if the political demands were met. A hypothesis is that the initial moves in Crimea were intended for coercive rather than separatist purposes. In his first statement, Putin said that he did not anticipate annexing Crimea and he may have been hoping for a much more generalized pro-Russian insurrection across eastern Ukraine. It was then that he gained authority from the Duma to send peacekeeping forces to Ukraine to protect Russian minorities. It was soon evident that only Crimea, where there was already a substantial Russian military presence, was in any sense under Moscow's control. On the 16th of March, a hastily arranged referendum supported the reintegration of Crimea into the Russian Federation and finally, on the 18th of March 2014, Russia managed to complete the annexation of Crimea (Freedman, 2014, p. 8-9).

So Russia succeeded in its conflict against Ukraine mainly by adapting a polymorphous HW policy based on the support from the vast majority of the Russians living in Ukraine. In a research held by professors John Laughlin and Gerard Toal was shown that the Crimean polity was strongly influenced by the Russian media while as many as 84% of ethnic Russians and Ukrainians in Crimea now support annexation. Furthermore the ratio of those who wanted to join Russia undoubtedly was convinced due to television-fed perceptions that ethnic Russians would become second-class citizens in Ukraine. On the other hand, unlike residents of western and central Ukraine who tend to readily self-identify in these terms, the strong majority (85%) of the population of Crimea do not perceive themselves as European (Kofman & Rojansky, 2015).

Also mistakes made by Kyiv's interim government in the aftermath of the Maidan Revolution, such as declaring a possible change to the status of the Russian language, or firing the Crimean Berkut (elite riot police) units, created additional opportunities for Russia. In addition to this, Russia's use of broadcasting tools for propaganda and psychological operations surprised both Ukraine and the West (Kofman & Rojansky, 2015).

The IW campaign in Ukraine entailed concerted use of Russian state-controlled media, due to the fact that Ukraine never contested the information space in Russian language programming, and so Russian media were able to quickly adjust their messaging in support of the Kremlin's objectives. Russia amped up the alarmist content of its broadcasting in response to the Maidan, stoking fear and confusion in Crimea, while at the same time broadcasts fell relatively flat in other regions of Ukraine, despite the fact that Russian state channels held the attention of most of the Russian speaking population (Kofman & Rojansky, 2015).

3.4 The Russian Hybrid Warfare

The Russian HW as it was stated in the previous paragraphs, is a very complicated and extended issue which can be categorized as follows:

A. Information Warfare

In Ukraine, the Russian military campaign on the ground was accompanied by an active media campaign that undermined Ukrainian authorities and their efforts to protect the country. Russian IO covered every layer of communication, targeting information assets in the physical, logical and societal domains as they were applied from the strategic to the tactical level in order to enable military actions by pro-Russian forces- by controlling broadcast and print media, shaped the narrative in the social media and isolated Crimea from independent news from abroad. The media isolation of Crimea was achieved by taking physical control of the Internet and telecommunications infrastructure and by disrupting cable connections. As a consequence, the target audience in Crimea shaped its perception mainly through Russian or pro-Russian media sources. Initially, Russia denied direct involvement. When the "little green men" appeared, both President Vladimir Putin and Defence Minister Sergei Shoigu denied the participation of Russian troops. It was in early March 2016, when Ukraine reported damaged fiber-optic cables, jamming of naval communications and defacement of government portals. Moreover mobile communications of government officials were compromised and news portals suffered distributed Denial of Service (DoS) attacks. Adding to that, a pro-Russian hacktivist group, Cyberberkut, managed to access phone recordings and electronic correspondence between Ukrainian, EU and US officials. Both governmental and private TV channels (e.g., Rossiya 1, NTV, Russia Today, LifeNews), radio stations (e.g., Radio Mayak), mobile phone operators (e.g., KyivStar), Internet sources (including online publications e.g., Itar Tass, RIA Novosti) and social media networks (e.g., YouTube, Facebook, Vk.com, odnoklassniki.ru) distributed Russia's disinformation and constructed a different narrative. The separatist People's Republics of Donetsk and Luhansk had their own channels producing anti-Ukrainian propaganda (e.g., dnr-news.com, novorus.info) (Kramer & Speranza, 2017, p. 21).

The narrative that the last 10 years Russia has constructed is framing Russia as a Eurasian power (a "new Great Russia") that must control Ukraine and the Black Sea, reviving somehow the powerful imperial Russia and the Soviet Union. According to this narrative, Ukraine has been an integral part of the Russian World since the birth of the Russian Empire and control over Crimea serves Russia's national interest, especially its' connection with the Sea Line Of Communication (SLOC) of the Black Sea. In order to support this fact, Russia exploited the deficiencies of the West and Ukraine, the political and economic crisis in Ukraine and urged the empowerment of nationalist and xenophobic trends that often occur in a crisis prone Ukraine that is divided between its pro-Russian population (Russophones), living mostly in the Eastern and Southern parts of Ukraine (depicted as Novorossiya), and pro-Ukrainians (Ukrainophones), who are situated in Western Ukraine (Kramer & Speranza, 2017, p. 21).

In the physical battlefield, during the Ukrainian crisis, Russia had more than 55,000 troops lined up on the Ukrainian border applying pressure. However, when instability had to be shown in Ukraine, non-conventional techniques were used: While the rebels directly engaged the Ukrainian army in the Donbass, the Russian military engaged in training exercises just inside Russian territory (Kramer & Speranza, 2017, p. 21).

B. Economic and para/side economic activities

On a parallel basis non-military instruments of Russia's hybrid concept have been brought to fruition via certain activities, shown its ability to use low-level force as a means to achieve numerous geopolitical objectives not only in Ukraine, but throughout Europe (Kramer & Speranza, 2017, p. 19):

- Investments in key sectors of European economies (e.g. lobbies in Great Britain, purchase of football teams such as Chelsea).
- The use of Russian investments, trade and capital in order to control key economic

and political elites (e.g. energy influence of EU-Nord Stream 1 and 2).

- Buy up media, support anti-integration and pro-Russian political parties.
- Sale arms to gain influence over military decision-making.
- Large-scale intelligence penetration of European organizations.
- Forging of links between Russian organized crime and local criminal elements.
- Establishment of ties among religious institutions, exploitation of unresolved ethnic tensions and campaigns for "minority rights".
- Massive coordinated cyber strikes on selected targets.

As with hybrid conflict in detail, Russia has employed a full spectrum of activities, ranging from incitement of violence, kidnapping and attempted assassination of political enemies of Putin's regime abroad (e.g. Scribal's case) to infiltration and covert action combined with military efforts. The Russian government has been accused of deploying operatives to foreign countries to deliberately protest or incite civil unrest or violence as part of its HW campaign. Higher on the scale of low-level use of force from incitement of violence is the capacity to breach borders, covertly or overtly, as part of a hybrid effort. For instance, in Estonia Russian forces crossed the border and kidnapped an Estonian border guard who subsequently was convicted by a Russian court and sentenced to a fifteen-year imprisonment for "spying, possession of weapons, and illegally crossing the border." Estonian officials pushed back citing Russia's clear violation of international law, highlighting that Kohver, the guard, was abducted on Estonian territory during "an audacious cross-border raid by the Federal Security Service of the Russian Federation (FSB) involving radio-jamming equipment and smoke grenades." Despite public calls from EU and other European officials for Kohver to be released, he was convicted and jailed in Russia, until returning to Estonia in a prisoner exchange (Kramer & Speranza, 2017, p. 19-20).

C) Operations in the Cyber domain

Russia has also the capability to utilize cyberattacks to disrupt operational networks (e.g. electric grids or finances) in both Europe and North America. The risk from cyberattacks to critical infrastructure is substantial. The former Director of National Intelligence James Clapper states that the telecommunications sector and the electric grid face escalating cyber threats to their Information Technology (IT), industrial control systems and other operational technology systems on which they rely (Kramer & Speranza, 2017).

Likewise, Admiral Michael Rogers, dual-hatted as the director of the National Security Agency and commander of Cyber Command, has come into the conclusion that energy firms and public utilities in many nations, including the USA, have had their networks compromised by state cyber actors.

Accordingly, vulnerabilities of Internet Service Providers (ISPs) (including Distributed Denial of Dervice (DDoS) attacks), in network devices and insider threats have been identified and telecommunications systems have been attacked in key European countries, including Poland and Norway. Finally, Ukraine’s electric grid was also targeted in an attack that disabled multiple distribution utilities and impacted over 200,000 people for several hours (Kramer & Speranza, 2017, p. 18-19 ; Abdyraeva, 2020, p. 22).

D) Application of political and other means

IW is not only conducted through cyber activities and media channels. As practice has shown, Kremlin also maintains influence through organizations and civil society, mainly through Russian and Russia-funded Government-Organized NonGovernmental Organizations (GONGOs) as part of a broader network designed to support Russian interests, propagate anti-Western narratives, undermine transatlantic values and institutions, and legitimize the Russian government’s actions by cultivating and coercing public support. For instance, when Russian politics refer to the Baltic countries, Kremlin uses *“the Russian-speaking minority and compatriot organizations to exert influence”* control the narrative, and shape public opinion (Kramer & Speranza, 2017).

The EU has strongly alleged that Russian used propaganda to interfere in important referendums in the Netherlands and Britain in 2016, including the Brexit vote. Russia has also been accused of interfering with the 2017 French presidential elections. The campaign manager of Emmanuel Macron accused RT and Sputnik of being “the first source of false information shared” about Macron. He also divulged that “during the same period, with the same rhythm,” the campaign has been a victim of hacks on its servers, as was undertaken just before the French presidential vote (Brattberg & Maurer, 2018).

Russia’s ability to combine disinformation efforts with cyberattacks has led to the emergence of hack-and release tactics that involve obtaining information and using it to influence public officials or opinion. US officials and analysts have asserted that this kind of Russian operation was behind the hack of the Democratic National Committee (DNC), and a broader attempt to influence the 2016 US presidential elections. In a joint statement in October, the US Intelligence Community explained that it was close to 100% sure that the Russian Government directed compromises of e-mails from US persons and institutions, including from US political organizations, and the thefts and disclosures were intended to interfere the US election process (Mueller, 2019). The continued referring that this kind of activities are not new to Moscow and have been used to influence public opinion across Europe and Eurasia (Mueller, 2019).*”*

The Russian government adopts a holistic approach to IW, which does not only affects the target state and its armed forces' ability to manage information and exercise effective command, but also achieves desired effects in the targeted populations' perceptions and decision making processes in favour of Russia's goals. Therefore, instead of conceptualizing cyber operations within the framework of cyber warfare, the Russian government includes them in the broader framework of its' IW.

Meanwhile, Russia's political and military officials have repeatedly denied the existence of Russian military operations in Ukraine since the beginning of the conflict. In January 2015, Russian Foreign Minister Sergey Lavrov responded to an accusation that Russian troops were in Ukraine by challenging publicly the presentation of facts for these allegations. (Rupert, 2015).

In his book about Soviet disinformation, a former Soviet intelligence officer and high-ranking defector, Pacepa, points out that a typical KGB campaign always involved the denial of its direct involvement. He writes that a three-pronged disinformation campaign precisely follows the rules of denying direct involvement in a situation, minimizing the damage and when the truth shows up, insisting that the enemy was wrong (Pacepa & Rychlak, 2013).

Not knowing Russia's true goals, the opponent is put in a position where he must guess them. For example, with its true goals concealed, Russia can threaten the enemy to provoke a costly response. In Ukraine, the strategy provides Russia with a wider set of strategic goals to choose from. If one approach fails, such as, presumably, Russia's initial intent to create a Ukrainian land bridge between Transnistria and Crimea – the enemy will not necessarily perceive it as a failure, ensuring Russia's image of superiority (Minzarari, 2022).

Such an approach also facilitates the Russian exit from Ukraine in case Russia decides that its military engagement is no longer required or desirable. If Russian troops are not officially in Ukraine, it is relatively easy to withdraw from the country without significant cost. Acknowledging Russia's presence in Ukraine might have forced international institutions to introduce a more severe punishment and might even have led to a full scale war. Instead, a consistent denial of Russia's military presence allows for more flexibility in resolving the Ukrainian crisis.

Putin has an affinity for juridism or the use of formal documents to justify his actions, as Fiona Hill and Cliff Gaddy argue in their book on the Russian leader. From a purely legal perspective, Russia's actions in Ukraine did not cross in 2014 and 2015 the threshold of international conflict despite ample evidence demonstrating Russia's military involvement in the country. Russia's actions in eastern Ukraine also fail to meet **the law of belligerent occupation**, which applies only when the following circumstances prevail:

- The existing government structures have been rendered incapable of exercising their normal authority.
- The occupying power is in a position to carry out the normal functions of government over the affected area (Hunter & Pernik, 2015, p. 3-4).

In order to prove that Russia is occupying eastern Ukraine it has to be proved that Kremlin wields overall control over this territory, not only by equipping and financing, but also by coordinating or helping in the general planning of its military activity. As a result, the documented degree of Russian involvement in Ukraine is insufficient to meet the overall control test. Although the evidence is enough to prove Russia finances and equips the pro-Russian separatists, it is insufficient to meet the requirements of organizing, coordinating and helping in planning military activities. So, from a purely legal perspective, the conflict between the Ukrainian government and the pro-Russian separatists is an internal conflict, not an international one. This strategy gives Russia enhanced influence in international organizations, as illustrated by the February 2015 "Minsk II" ceasefire agreement. Russia, as one of the signatories of "Minsk II", does not formally have any obligations to fulfill the agreement, while Ukraine has to fulfill a lot of responsibilities

(Hunter & Pernik, 2015, p. 3-4).

3.5 Conclusion

The “Russian” model of HW is different from the Western/NATO one. Analysis has identified three stages:

- Destabilizing a country via inspiring domestic conflict.
- Causing state collapse via ruining economy and destroying infrastructure.
- Replacing local political leadership with own influenced operatives (Freedman, 2014).

Russia’s convergence of a variety of tactics referring to HW are the means to accomplishing a broader strategy meeting the following goals:

- Recreation of a Russian empire (“Novorussia” or “New Russia”).
- Stop the EU’s ability to control energy pipelines.
- Weaken and divide the West reflecting somehow realist goals of a former, less inter-connected world (Liaropoulos, 2019, p. 197).

The Western refrain that economic interdependence is a means of preventing conflict is much less of a factor in President Vladimir Putin’s rationale than expected. In an interview with BuzzFeed, the former US President Barack Obama said about Putin’s world view that Putin looks at problems from a Cold War’s perspective and so he has missed some opportunities for Russia to diversify its economy, to strengthen its relationship with its neighbors and to represent a more friendly attitude (Hunter & Pernik, 2015, p. 3).

On the tactical level, IW allows Russia to achieve surprise in the time or manner of an attack. Russia thereby gains time and efficiency against the enemy’s ground forces. Since the conflict in Ukraine in 2014 was not declared as war and the separatists conducted high-intensity operations in short bursts, the enemy was taken by surprise and was presented with an erroneous image of the situation. This factor helped Russia’s successful operation in Crimea with very few casualties. However, as the West understands Russia’s tactics better, the advantage of novelty in Russia’s approach to Crimea is less likely to benefit its next political-hybrid adventure (Liaropoulos, 2019, p. 196-197).

The informational cover also offers the military aspect more autonomy when the greater precision of the troops is in higher demand than ever before in Russian history. Spetsnaz, like the VDV Airborne troops of the Naval Infantry marines, represent an army within an army able to operate professionally, decisively and covertly.

Further development of such tactics could allow Russia to reduce the numbers of troops and the amount of equipment used in operations, according to Bedritsky, passing successfully one of its' numerous military reforms in history. Consequently, Russia will also be able to manage defense expenditures, while limiting the enemy's capacity to counter compact, dispersed units. It will also permit Russia to avoid clashes with heavily armed, but less mobile parts of the enemy and quickly neutralize or eliminate these units' command structures.

Finally, among the key lessons learned from the 2014 Russia-Ukraine conflict and its HW tactics are:

- Mixed ethnic societies are particularly susceptible to mass and social media manipulation.
- Prior to conflict, subtle economic influence and the promotion of corruption serve to establish leverage.
- Political agents, volunteers and mercenaries provide a variety of low visible sabotage and advisory options.
- Use of terrorist type techniques.
- Low-intensity conflicts that escalate rapidly to high-intensity warfare unveil unpreparedness of police, border guards, security units and even SOF teams to deal with these challenges.
- A variety of subtle and direct nuclear threats, including nuclear alerts (e.g. Zaporizya nuclear energy factory) reopen the nuclear debate.

CHAPTER 4

Non State actors: Israel vs Hezbollah case study

4.1 Introduction

An additive fact of the complexity of HW is that it can be conducted also by Non State actors which are basically terrorist and paramilitary groups. Non-State HW originally appeared on the battlefield in places like Lebanon and later in Afghanistan and Iraq. The term "hybrid" in this non-state actor context was used to illustrate how actors such as Hezbollah combined the characteristics of unconventional and conventional warfare with other non-military modes of operation in novel and unfamiliar ways that challenged both Western military practice and strategic thinking (especially by the need to change the strategic doctrines of many countries such as USA and Israel) (Reichborn-Kjennerud & Cullen, 2016, p. 1).

Various characteristics have been attributed to HW conducted by non-state actors:

- Increased levels of military sophistication as they move up the capabilities ladder, successfully deploying modern weapons systems, technologies and tactics traditionally understood as being beyond the reach of non state adversaries.
- Expansion of the battlefield beyond the purely military realm, along with the growing importance of non military tools. From the perspective of the non state actor, this is a form of horizontal escalation that provides asymmetric advantages to non state actors in a conflict with militarily superior state actors.

Through an incorporation of the diverse characteristics of state and non-state HW, based upon a number of certain characteristics (asymmetric and multi-modal, along with a horizontal and a vertical axis) and to varying degrees shares an increased emphasis on creativity and ambiguity that leads to the following model (Figure 6) which describes how a HW actor uses its instruments of Military, Political, Economic, Civilian and Informational (MPECI) power across the Political, Military, Economic, Societal, Informational and Infrastructure (PMESII) vulnerabilities of a target system, to escalate – vertically and horizontally – in order to achieve the desired goals (Reichborn-Kjennerud & Cullen, 2016, p. 1).

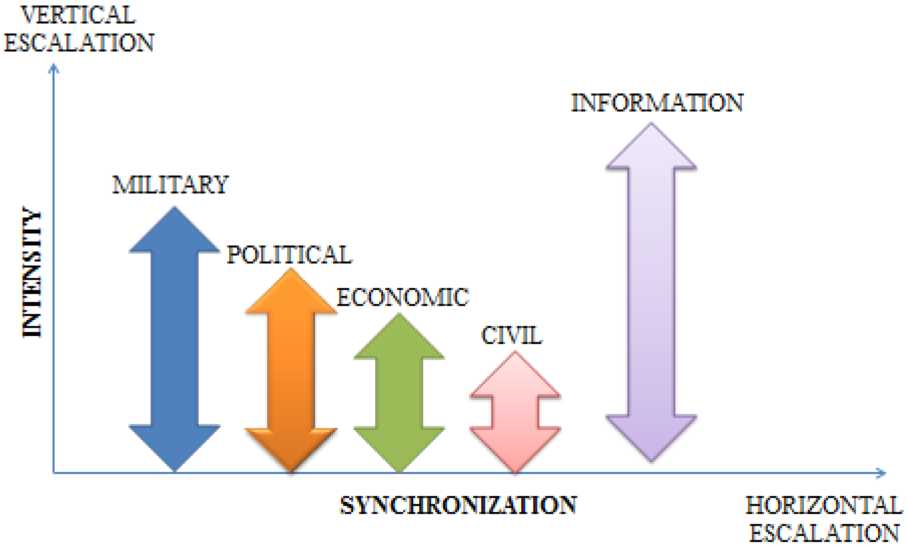

Figure 6: MPECI diagram

Source: (Reichborn-Kjennerud & Cullen, 2016)

As it has been underlined before, HW is characterized by the tailored use of all instruments of power against the vulnerabilities of the opponent's system. These instruments can be divided into the more traditional MPECI categories, but will be used in synchronized and coordinated fashion against the opponent's system CoG, critical functions and vulnerabilities (PMESII) in order to have a change in the behavioral or physical state of a system according to the desired political goals. So, by implementing the definitions of **Vertical and Horizontal escalation**, HW refers not only to the means but also to how these are employed in a highly coordinated and synchronized fashion to create synergistic effects beyond the immediate element of power. This synchronization has the effect of acting as a force multiplier. This, in turn, assumes that HW requires a high degree of centralized operational command, control and strategic coordination of the elements of power, which can also be applied on the tactical level of a conflict. As Figure 6 describes, the means (the elements of power) may be vertically escalated or de-escalated (increased/decreased intensity), or horizontally escalated or de-escalated (synchronization of elements of power creating effects that can have the same impact as vertical escalation of one mean) – or a combination of the two, to achieve a goal. For instance, one could vertically escalate the political spectrum of the PMESII while horizontally escalating into other spectrums such as the informational and military. By employing all elements of national power, the ability to escalate vertically and horizontally increases, and thus also the ability to create effects (Reichborn-Kjennerud & Cullen, 2016, p. 3).

Bearing in mind the above analysis, it could be easily understood how important is the study of historical conflicts, such as the second Lebanon war, in which every aspect and mean of the HW context was applied.

4.2 Historic and religious background of Hezbollah

Hezbollah is a Shia Muslim political group with a militant wing which is called the Islamic Resistance. Its' main presence is situated in Lebanon acting as a "state-within-a-state", being also a major provider of social services, operating schools, hospitals and agricultural services for thousands of Lebanese Shias. It has been present in the Lebanese political system since 1992, increasing its' power over the recent years from two to eleven out of thirty seats in the Lebanese national unity cabinet. In addition to this, it has installed and uses a satellite TV channel (*"al Manar"*) and a broadcast station (both regarded as terrorist entities from the West). Ideological and financial support for the organization is provided by Iran and Syria and also raises funds from criminal activities, such as counterfeiting money, drug production and trade. Consequently, Hezbollah concentrates all the characteristics of a non state actor, according to the MPECI diagram later described, that can conduct on a large scale a HW (McCulloh & Johnson, 2013, p. 21 ; Huovinen, 2011, p. 24).

Hezbollah's first appearance was in the late 1970's as a result of the Lebanese Civil War (1975-1977) and the two Israeli campaigns in Lebanon in 1978 and 1982, countering the action of the Amal Movement, which was the largest Shia organization in Lebanon at that time, and separating its' role from Palestine Liberation Organization (PLO) or other Palestinian groups operating in the area. Responding to the Israeli invasion of Lebanon, in 1982, the abovementioned group of Lebanese Shia Muslims declared themselves to be the *"Party of God" (Hizb Allah)* and so Islamic resistance units were formed and committed to the liberation of the occupied territories and the ejection of the Israel Defence Forces (IDF) which intended to stay in South Lebanon. Hezbollah was assisted both ideologically and logistically by the Iranian Revolutionary Guards based in Lebanon's Bekaa Valley, another reason why Hezbollah draws inspiration form the Iranian Revolution, having as endmost goal the creation of an Iranian style Islamic republic in Lebanon, strongly anti-Western and anti-Israel, removing also all the non-Islamic influences from its' territory. Being both of them Shia Muslims, the ideological connection between Iran and Hezbollah has always been strong. Since Hezbollah was founded it has received support from Iran and Syria, both financially and in military training (McCulloh & Johnson, 2013, p. 21 ; Huovinen, 2011, p. 24).

As it was stated before, Hezbollah is a Shia Muslim organization in which religion plays an important political role. They differ from Sunni Muslims in the perspective of leadership and not in the spiritual aspect of religion, believing that their leadership, either religious or political, descend directly from the family of the Prophet Mohammad or God himself. Therefore among the Shias, Imams are considered sinless by nature and their authority infallible since it comes directly from God or the family of the Prophet. Hence the leaders are highly respected, and their authority unquestioned. Among the Muslims worldwide, Shias are a minority with about 15% of the Muslim population worldwide. The attitude towards the divine authority of Shia Imam's explains how Shia organizations may turn extremist and be considered to behave like terrorist organizations from the West point of view (Huovinen, 2011, p. 25).

Moreover, Hezbollah is by its nature asymmetric and has potential for conventionality. Developments in Hezbollah since the Second Lebanon war indicate a potential to strategically align with forces seeking to contest USA military presence in the Middle East and beyond, showing also an immense capacity for doing whatever is needed to survive. Many consider this pragmatic, but Shia Islamic doctrine allows for deception and false alliances, allowing thus Hezbollah to do things that look pragmatic on the surface, but which are entirely in accordance with Shia doctrine. For example, they can ally with

Christians in parliament, deal with infidel regimes such as North Korea, traffic drugs in the Latin American Tri-border area, and still be good Muslims waging true jihad. Yet, Hezbollah maintains significant funding streams from North Africa, the USA and Latin America, essentially anywhere a Lebanese diaspora exists. Additionally, they have relations with North Korea for their tunnel building consultation along with numerous regional entities such as Sunni Hamas (Huovinen, 2011, p. 25).

Having to do with the religious-political aspect, Hezbollah's interests are to maintain the armed Hezbollah militia. This allows them to honor their first obligation: ***Jihad against the Zionist entity without Lebanon being held accountable militarily***. Another point is that they seek to maintain as influential a presence as possible in the Lebanese political sphere without becoming the state. By being a de-facto veto entity in the Lebanese parliament, they reap the benefits of political power without the responsibilities of governance. Also, Hezbollah stays true to its' primary Shia religious concepts: ***Loyalty to the Iranian Leader, Jihad and Shihada (martyrdom)***. Finally, they seek to develop depth by refining and bolstering relationships for funding and support with other states such as Syria (McCulloh & Johnson, 2013 ; Huovinen, 2011).

4.3Military Campaigns of Hezbollah

Once established as a militia, Hezbollah received acclaim and legitimacy in Lebanon and throughout the Muslim world by fighting against the IDF and the South Lebanese Army (SLA). Its base areas were, and still are, Lebanon's Shiite dominated areas, parts of Beirut, Southern Lebanon and Bekaa Valley. Aside from its activities in Lebanon, in 1980's and early 1990's Hezbollah conducted a global terrorist strategy with a capability to operate all over the world, and they carried out terrorist attacks against Israeli and US targets, focusing mainly on South America, Southeast Asia, Jordan, the Persian Gulf, and the European continent (Johnson, 2010, p. 2-5).

As a result, Hezbollah was responsible for a series of terrorist attacks against Western targets such as:

- Suicide bombings of the U.S. embassy (1983), U.S. Marines base (1983), the U.S.

Embassy Annex in Beirut (1984).

- Aircraft hijackings (Trans World Airlines 1985, Kuwaiti Airlines 1984 and 1988), the attack on Israeli Embassy in Argentina (1992).
- Kidnappings of U.S. and European civilians as well as French, British, German and Russian diplomats. Hezbollah was responsible for most of the kidnappings of foreign nationals carried out in Lebanon during that time period (at least 18 citizens of Western countries were held hostage, and three of them were killed) (Huovinen, 2011, p. 26).

In the 1990's, following a shift in Iranian policy, Hezbollah lowered the profile of its anti-Western pursuits and focused its attention on terrorist activity against Israeli targets. In 1989, heavily influenced by Syria, the Lebanese administration accepted Hezbollah as the only militia organization in Lebanon, whereas all other ethnic militias were to be dismantled. Along with the weakness of the Lebanese central regime, Hezbollah's special status enabled the organization to use its power and seize both military and civilian control in Southern Lebanon (and several areas of the Bekaa region), practically replacing the legitimate Lebanese regime. This process continued even after the IDF withdrawal from Lebanon. Southern Lebanon had in fact turned into a state-within-a-state as it was abovementioned. Hezbollah thus became the ultimate authority in this region, while the Lebanese regime focused mainly on economic development projects that were approved by Hezbollah. Moreover, Hezbollah pursued its own policy in southern Lebanon, which was imposed on the Lebanese government, opposing the effective deployment of the Lebanese army in the south thus preventing the Lebanese regime from assuming responsibility for this region's security. According to the resolution 425 of the United Nations (UN) Security Council, the Lebanese army had to be deployed in the south of the country, but by receiving strong support from Syria, Hezbollah openly rejected this mandate and carried on as before (Huovinen, 2011, p. 27).

As an ethnic-religious feature, the Shia community had been the largest, and yet the most underprivileged ethnic community in Lebanon. For Hezbollah this created a fertile soil for gaining support with an extensive social and economic program, since the central government was unable to improve the situation. Far-reaching social and welfare activities were carried out by Hezbollah, including schools, women's affairs, health and medical services, social welfare and religious education, actions that were financed by the funds received from international fundraisers and its support from Iran and Syria. Inevitably, Hezbollah earned the trust and support of the Shia community as well as some non-Shias, gaining that way political power in Lebanon in its' pursuit of forming an Islamic republic in Lebanon (Huovinen, 2011, p. 27).

In the beginning of the 21st century, there was an increasing cooperation between Hezbollah and other Palestinian terrorist organizations in the region, being really active against the IDF during the withdrawal of Israeli forces from Lebanon in May 2000 after the termination of the Second Lebanese Civil war (1985-2000). Focus was transferred to violent activities in Israeli territory with the aim to disrupt any attempt at dialogue and peace process in general. However, since the 11th of September 2001 attacks Hezbollah made considerable efforts to promote its image in order to blur its identity as a terrorist organization, denying publicly its involvement in terrorism in general, and in particular. Yet despite the Israel's withdrawal from Lebanon in 2000, Hezbollah continued periodically to shell Israeli forces in the disputed Sheba Farms border zone resulting periodic conflict and a retaliation from Israel. In the end of 2005, Hezbollah and the IDF had a heavy exchange of fire across the Blue Line established by the UN Security Council resolutions 425 and 426 for the IDF withdrawal from Lebanon in 2000. Both sides used heavy weapons against each other (Huovinen, 2011, p. 28).

After the withdrawal of IDF from Lebanon in 2000, Hezbollah kept close ties to Iran and Syria and began arming itself, mainly with High quality weapons, such as land-to-land rockets, anti-tank weapons, anti-aircraft missiles, mines and mortar rounds as well as explosives, small arms and ammunition. In September 2004 the UN Security Council resolution 1559 called for the Lebanese government to disband and disarm all Lebanese and non-Lebanese militias and to prevent the flow of armaments and other military equipment to the militias from Syria, Iran and other nations. The Lebanese government did not comply with the resolution because Hezbollah was very popular among the Shiites, it had built a considerable military strength and it did not want the Lebanese army in the Southern Lebanon/Hezbollah's territory. Furthermore to this situation, the November 2005 clash between Hezbollah and IDF, in its shortness and intensity, was like a prologue to the Second Lebanon War the following year. The military and financial support Hezbollah received from Iran and Syria did not go unnoticed by the international community, forcing the UN Secretary General Kofi Annan on April 2006 to demand from Syria and Iran to stop interfering in Lebanon (Huovinen, 2011, p. 28).

4.4 The Second Lebanese War

4.4.1 Political Background and Strategic Level

The Second Lebanese War (2006) was a 34-day military conflict, between the pre-eminent conventional military force in the Middle East—Israel—against the combined conventional and unconventional military force of the non-state actor Lebanese Hezbollah. The conflict began when Lebanese Hezbollah conducted attacks against Israeli border forces and kidnapped two Israeli soldiers on the 12th of July 2006. Israel responded with a failed rescue attempt and a synchronized air and ground bombardment of Southern Lebanon, followed by a ground invasion and a naval blockade of Lebanon. Lebanese Hezbollah retaliated with massive rocket strikes into Northern Israel and a guerilla campaign utilizing prepared, hardened defensive positions. Fighting continued until regional and international pressure resulted in a United Nations brokered ceasefire on the 14th of August 2006 (Hoffman, 2009, p. 37 ; Pana, 2016, p. 68).

In total, the fighting resulted in the deaths of approximately 1,200 people. The fighting displaced over a million people in Southern Lebanon and in Northern Israel. On the Israeli side, 114 IDF soldiers were killed and significant amounts of Israeli military equipment were damaged or destroyed, including up to 10 percent of Israel's committed main battle tanks, some rotary wing aircraft and coastal naval vessels. More than 40 Israeli civilians were killed and nearly 4,000 were injured in addition to an estimated $3.5 billion loss in war cost and economic output. Accordingly, in Lebanon, Hezbollah suffered contentious losses of between 46 and 600 fighters killed, and its observed military capability was estimated to have been reduced by one half. In addition, over 1,000 Lebanese civilians were reportedly killed and over 4,000 were injured in addition to an estimated $4 billion loss in buildings and infrastructure. This conflict played out against a historical backdrop of political, religious, and ethnic tensions between the strong state actor, Israel, and the ambiguous non-state actor, Lebanese-Hezbollah within the neighboring weak state of Lebanon. Israel is a strong, Jewish state in a contested geographic area, historically fighting for survival against the Arab and Muslim populations of the Middle East for more than 70 years. Israel's state is consisted by a dominant Jewish demographic characteristic and is supported by a strong internal economy and external remittances, influencing on a parallel line the strongest economic and political lobbies of USA, Great Britain, France, e.t.c. . In addition to this, Israel's military industrial complex is the most advanced within the Middle East region, fielding advanced ground, air and sea platforms and simultaneously exporting high level technological knowhow worldwide (McCulloh & Johnson, 2013, p. 20).

On the other side, Lebanon is a multicultural weak state, which has been a confluence of both Middle Eastern and Mediterranean population and beliefs for centuries. This cultural milieu has resulted in a demographic mix that tentatively balances between multiple Muslim and Christian factions within the habitants. As a result, Lebanon has a relatively weak central government and with control distributed among many factions according to the 1926 Lebanon Constitution. During the civil war of 1975-1990, this balance of power was contested. Following the 1979 Iranian Islamic Revolution, additional pressure was placed on the balance of power via the Shi'a demographic. This in turn has led to external interference and sometimes domination of Lebanon by her stronger neighbors, Syria and Israel—perpetuating the cycle of lack of control and resulting in historically poor infrastructure, which is the following state of its old colony status by France. The weak governmental structure is mirrored by a relatively weak military that lacks not only the power to conduct external defense, but also to impose or support internal order—effectively creating an internal power vacuum, which is the actual reason of the United Nations Interim Force In Lebanon (UNIFIL) deployment since 2006 serving in order to assist Lebanon in creating strong and independent Army and Police Forces. Hezbollah filled the power vacuum created by this lack of internal political and military strength in the early 1980s as it was stated before. As a result, the unique picture of Lebanese Hezbollah is built to show its attributes as a hybrid organization (McCulloh & Johnson, 2013, p. 20-21).

4.4.2 Operational Level

The comparison between IDF and Hezbollah through the principles of HW shows clearly the reason why Hezbollah used this kind of strategic and operational doctrine during the war (McCulloh & Johnson, 2013, p. 20):

- A hybrid force's composition, capabilities, and effects are unique to the force's own specific context. This context includes the temporal, geographic, socio-cultural and historical setting in which the given conflict takes place. Lebanese Hezbollah exists within just such a specific enabling context. The weak central government and conflicted lines of power within the country allow Lebanese Hezbollah to exist peaceably, maintaining and improving its militant status and freedom of action. Lebanon itself is not only a cultural and demographic mix of Eastern and Western society, but it also rests within the arc of a large Shi'a Muslim demographic density that extends from Lebanon through Syria, Iraq, Iran, and Bahrain—otherwise known as the *"Shi'a Crescent"* which serves to unify Lebanon's internal Shi'a Muslim population allowing Lebanese Hezbollah a solid base of support. In addition, the ideology espoused by Lebanese Hezbollah extends to the Lebanese diaspora throughout the world and engenders both sympathy and support for the organization (McCulloh & Johnson, 2013, p. 21).
- A specific ideology exists within the hybrid force that creates an internal narrative to the organization. This ideology inherently links to the strategic context and is grounded within the socio-cultural, religious identity of the hybrid force. The resulting narrative redefines the extant rules within the strategic context. Hezbollah maintains an ideology of **righteous** Islamic Revolution grounded in both its assumed role as an anti-Israeli militia and as a Shi'a protector in Lebanon. This narrative supports both the external and internal support relationships as well as facilitating the growth and control requirements of Lebanese Hezbollah, pointing out also the inadequacy of the Lebanese government (McCulloh & Johnson, 2013, p. 22).
- Hybrid force's perception of an existential threat by a potential adversary. This perceived threat drives the hybrid force to abandon conventional military wisdom in order to find ways to achieve long-term survival. In the case of Lebanese Hezbollah, Israel established a long historical precedent of military action and occupation in Lebanon in 1948 during the Arab-Israeli War with the Israeli occupation of numerous southern border villages in Lebanon. The invasion of southern Lebanon followed in 1978 and occupation of territory south of the Litani River. In 1982, a large Israeli ground force briefly entered the eastern portion of Beirut, the capital of Lebanon. The Lebanese people and Lebanese Hezbollah can

see Israel as an existential threat if it combines selected historical facts with Israeli policy statements. Actually, Lebanese Hezbollah's public rhetoric regularly incorporates this narrative. The realization of this existential threat thereby prompts Lebanese Hezbollah to seek any method possible to defend itself—including both conventional and unconventional methods. Another result of this rhetoric is the tacit approval of the Lebanese people—which creates a support base that enables the actions of Lebanese Hezbollah (McCulloh & Johnson, 2013, p. 22).

- During a HW exists a capability overmatch between the hybrid force and a potential adversary. The hybrid force contains less conventional military capability compared to its adversary and therefore must seek a way to offset this apparent advantage in military capability. In the case of Lebanese Hezbollah and Israel, this overmatch is readily apparent. Israel not only maintains a large internal military industrial complex, but also links through close alliances to both the American and European military industrial complexes. Lebanese Hezbollah on the other hand, maintains an ad-hoc militia force that is reliant on external arms supplies and unconventional techniques, having a strong knowledge of guerilla and urban warfare tactics (McCulloh & Johnson, 2013, p. 22-23).
- However, a hybrid force contains both conventional and unconventional elements (that's why it is called **hybrid**). These elements often comprise "accepted" military technology and nonmilitary, guerrilla type technology and tactical application. These combined capabilities create an asymmetric advantage for the hybrid force. In a ground force comparison of the 2006 War, Israel fields an army containing main battle tanks such as the Sabra Mark I and Merkava Mark IV, armored personnel carriers like the Namer, infantry fighting vehicles such as the Golan Armored Vehicle, towed and self-propelled artillery systems like the LAROM and Sholef, and multiple variations of Unmanned Aerial Vehicles (UAVs). Additionally, Israel maintains multiple air force strike fighters such as the Kfir and F-16I, rotary wing platforms, and coastal defense ships. On the other side, Lebanese Hezbollah utilizes multiple small arms variants, anti-tank munitions, anti-aircraft systems, anti-ship weapon systems, and multiple rocket and missile platforms. Conventional fighters were capable of advanced application of their weapon systems, as seen in the example of 3709 rocket attacks

launched into Northern Israel (hitting 901 towns and cities during the Second Lebanon War), while irregular militia units used Improvised Explosive Devices (IEDs) and were capable of near simultaneous swarming attacks (McCulloh & Johnson, 2013, p. 23).

- Hybrid forces seek to use defensive type operations, create ambushes and quick counter attacks. This kind of operations will often include offensive components, but the overarching intent will still be one of defense. In the 2006 Israel-Lebanese Hezbollah War, Lebanese Hezbollah fought from prepared fighting positions, including fortified bunkers, which were arranged in depth in Southern Lebanon, which was a terrain that they knew and had done site surveys numerous times. From these defensive positions, Lebanese Hezbollah launched multiple rocket attacks and executed swarming attacks against Israeli ground forces. As such, these operations primarily focused on the overall survival of Lebanese Hezbollah forces or on the protection of their corresponding local support networks. In general, all ground engagements occurred when IDF entered into areas occupied by Lebanese Hezbollah fighters. Rocket attacks were offensive in nature, but were launched for the stated purpose of retaliatory strikes against Israeli forces in Lebanon in the context of contested areas such as Shaba Farms or the Golan Heights and as such can be viewed as overall defensive operations which could also help in the breaking of the IDF's chain of C4 between army groups posing psychological effects upon them. Lebanese Hezbollah relied on attritional tactics throughout the Israel-Lebanon 2006 War, consonant with the HW theory (McCulloh & Johnson, 2013, p. 23-24).
- Finally, the use of attritional tactics in the employment of the hybrid force. In the case of Lebanese Hezbollah, the physical manifestation of these attritional tactics occurred using mine and improvised mine warfare, mass use of indirect fire attacks—missiles, rockets, and mortar fire, and the use of anti-tank/anti-personnel ground ambushes. As such, Lebanese Hezbollah rarely massed outside of occasional swarming attacks which were multi-directional. Additional moves were the cognitive aspects of attritional tactics in the use of the initial kidnapping of two IDF soldiers, threats of suicide bombing, the repeated bombardment of Israeli civilian populations and the rapid use of media to execute strategic information influencing operations(McCulloh & Johnson, 2013, p. 24).

Although Lebanese Hezbollah received more damage than the IDF and was tactically defeated on multiple occasions throughout the 34-day conflict, Lebanese Hezbollah was able to take advantage of several critical factors in order to gain an operational and strategic victory. Despite their clear military and economic advantages, the IDF were unable to meet the operational and strategic objectives that needed in order to military defeat the Lebanese Hezbollah, therefore the majority of public opinion in Israel, Lebanon and throughout the world saw Israel as losing the conflict. As a hybrid force, Lebanese Hezbollah was able to use its internal strengths of narrative, mix of weapons and tactics and by optimizing its military organization scheme against a Western style conventional military organization succeeded to overcome its' weaknesses and fight against a much stronger opponent. Thus it needed a combination of available equipment like anti-tank, anti-aircraft, anti-ship, and unconventional weapons—IEDs—and flexible defensive tactics like fortified defense in depth and ambush type tactics. This was coupled with an adaptive use of media exploitation and messaging in combination with a near continuous rocket bombardment. In doing so, Lebanese Hezbollah was able to bind the strategic objective of victory within the internal narrative of a Shi'a protector fighting against the existential threat of Israel. As a result, Lebanese Hezbollah acted as an agile, adaptive, and lethal opponent that only had to continue to fight in order to achieve its objective and defeat its enemy. In this sense, the hybrid force gained a clear advantage through synergistic effects and achieved the desirable "victory" (McCulloh & Johnson, 2013, p. 25).

4.4.3Phases of the Conflict

The 34-day long Second Lebanon War was initiated by the kidnapping of two Israeli soldiers by Hezbollah near Shtula on the Lebanese-Israeli border on the 12th of July 2006. The kidnapping Hezbollah unit had crossed the border during a diversion attack of Katyusha rockets and mortar rounds against the border villages and IDF positions. Israel responded and launched a large-scale **retaliatory** operation which eventually escalated into a war. The war that ended in a ceasefire agreement on August 13, 2006, can be divided into three phases:

- **Phase I:** Air campaign (July 12-16).

- **Phase II:** Engagement of ground forces (July 18 – August 11).
- **Phase III:** Final push (August 12-13) (Huovinen, 2011, p. 28).

The first phase of the Israeli retaliatory operation began with a massive use of Israel Air Force (IAF). On a parallel line IDF imposed air and sea blockades on Lebanon as the IAF attacked suspected Hezbollah command posts in Beirut, including military targets along the Beirut – Damascus highway and elsewhere, trying eventually to destroy the long-range missile launchers used by Hezbollah against Northern Israel. Israel refrained from bombing Lebanese infrastructure, although the IDF Chief of Staff, Lieutenant General Halutz had suggested that, imposing that way itself restrictions to conduct the operation. Additionally, Israel avoided a direct confrontation with Syria, despite the support it gave to Hezbollah. Within the first two days of the war, the IAF destroyed most of the Hezbollah's medium and long-range missile launchers, along with the Hezbollah command centres in Beirut. Yet the Israeli retaliatory campaign met an unexpected surprise, when the missile corvette INS Hanith, was hit with an anti-ship missile fired by Hezbollah, as she was monitoring the imposed naval blockade, conducting a massive psychological and operational hit against Israel. Then, Lebanese government asked for a ceasefire on July 14, which was turned down few days later (Huovinen, 2011, p. 28).

A significant point of study is that in the beginning of the operation the Israeli political and military leadership was both confused and indecisive of the objectives and methods to reach them. For instance, the IDF Chief of Staff was initially thinking as the operation would be a retaliatory attack and not war, instructing also his subordinates at the General Staff level not to use the term "war" regarding the operation. Finally Israel had five main objectives in the war and generally in its strategic and political doctrine in the Middle East region:

- Destroy the "Iranian Western Command" before Iran being able to use nuclear power.
- Restore credibility of Israeli deterrence after the withdrawals from Lebanon (2000) and Gaza (2005).
- Try to force Lebanon to act as an accountable state, including the end of Hezbollah's "state-with-in-state" status.
- Damage or cripple Hezbollah although it would continue to be a major political player in Lebanon.

- Bring back to homeland the two kidnapped soldiers without major trades of prisoners held by Israel (Huovinen, 2011, p. 29).

Even though the operation was initially thought to be carried out mainly on an air campaign, a reserve infantry division was mobilized as early as on the 13th of July, followed by three more infantry. Regardless of the damage inflicted on the Hezbollah long-range missiles and launcher arsenal, Hezbollah still had the capability to fire hundreds of short-range rockets a day into Northern Israel. This caused serious infrastructure and moral damage to the Israeli civilian population living in the area. It was now finally understood by Israel’s political and military leadership that the war could not be won without the ground element, and it felt forced to apply ground forces into battle, having as main task the destruction of Hezbollah’s positions along the Israel-Lebanon border (Huovinen, 2011, p. 30).

On the 22nd of July, the second phase began with IDF applying ground forces in battle in Southern Lebanon. The Israeli forces fired against the Hezbollah forces in Southern Lebanon, uncharacteristically to its tradition of mechanized warfare of outflanking and encircling the enemy, including the use of the element of surprise. The audacious fighting capabilities of Hezbollah came as a surprise to the troops on the ground, putting into consideration the effectiveness of the Israeli intelligence service. The Israeli troops on the ground faced an enemy with well prepared defence lines and bunker systems, well armed troops with missiles, rockets and advanced lighter arms like anti-tank weapons and surface-to-air missiles. Numerous short range rockets were launched by Hezbollah which terrorized the civilian population in Northern Israel and stopped the quick and steady movement of the Israeli land forces. However, the IDF operations kept building up and on the 29th of July an increased effort by the Israeli’s was made in order to create a security belt on the Northern Lebanese border. The ground troops took hold of dominating terrain and Special Forces hit targets in Bekaa Valley and Tyre, but had not much overall result (Huovinen, 2011, p. 30).

An obvious characteristic of the Second Lebanon War was that IDF often faced Hezbollah in urban areas, where Hezbollah had already built its bases there. It used civilian facilities and homes to store weapons and supplies and for fighting positions. Rockets and mortars were deployed within towns and homes, with the Hezbollah soldiers rushing in and out to carry out firing missions. They also used the people of Lebanon as human shields for their advantage, clearly against the rules of the international laws of war. IDF faced the challenge of target intelligence and collateral damage:

- How to verify targets to be engaged with different types of weapons and how to avoid collateral damage?
- How much to limit the strikes and the use of force, if military operations were carried out of civilian facilities, or in the immediate vicinity of them?
- On the other hand, if the IDF Chief of Staff had publicly stated a threat of "setting Lebanon back 20 years", it is tempting, if not evitable, for a non-state actor with terrorist status to use civilians as human shields.
- Collateral damage would be beneficial for Hezbollah as an excellent media operations material to bring the population on their side as Hezbollah's leadership used effectively its own TV and broadcast capabilities to send out their own message in every single point of the world (Huovinen, 2011, p. 31).

Another characteristic of Hezbollah fighting during the conflict was their well trained soldier's use of the advanced weapon systems they had acquired before the war, such as anti-tank weapons, anti-aircraft missiles, anti-ship missiles and UAVs. The anti-tank weapons were used skillfully in terms of tactics as multiple rounds were fired at the same target indicating that the use of anti-tank weapons was concentrated in anticipated kill zones. In addition to this, anti-tank weapons were effectively used against IDF ground troops seeking protection from buildings, causing most of the casualties of IDF in the war. The anti-aircraft missile capability, played an important role from the Hezbollah's perspective, although it destroyed only one IAF aircraft during the war, because, just the knowledge of short range air defense missiles possessed by Hezbollah forced IAF to change mission profiles and to use extensively countermeasures to avoid possible ambushes to IAF planes (Huovinen, 2011, p. 31).

In the first days of the war Hezbollah damaged INS Hanith with an anti-ship missile, a capability thought to be possessed only by national armies rather than by an organization with terrorist status. Israeli intelligence had given estimates of such weapons in the possession of Hezbollah as early as 2003, but the Israel Navy did not take the warning seriously and as a result missile corvette INS Hanith operated without using active countermeasures (Huovinen, 2011, p. 32).

The UAVs supplied by Iran provided Hezbollah with another force multiplier. With a range of up to 450 kilometers and payload capability of 45 kg it could deliver its load practically anywhere in Israel with an accuracy of 10 m with the Global Position System (GPS) guidance system. One penetrated Israeli air defense system and was shot down by IAF 15 km from Haifa. This demonstrated a new threat to Israel, since the UAVs could not be detected with the normal surveillance radars and with new effects unimaginable if its payload had been chemical or biological bombs. Although the long and medium range rockets and missiles threat to Israel was dismissed by IAF during the first days of the war, Hezbollah demonstrated its capability to cause damage and continuously threat the Northern Israel civilian population by the firing of short range rockets. The smaller rockets required smaller launchers, so they were moved and hidden easily and were both quick to set up and fire – a weapon that was used very effectively. There were some reports supporting that Iran promoted Electronic Warfare (EW) capabilities of Hezbollah during the war, such as jamming and successful hacking of Israeli communication, which Israel has denied. It can be said that Hezbollah was well prepared to fight the war under the influence of Israeli EW and could maintain its C2 structure throughout the war (Huovinen, 2011, p. 32).

Due to the ineffectiveness of the IDF in the battlefield against Hezbollah's ground positions in Southern Lebanon, and particularly the IAF's inability in handling the continuous short-range rocket launcher threat to Northern Israel, it became evident that unless the territory from where the rockets were launched was captured, the threat would be constant. This set the stage for the third phase for the war. Although cease fire negotiations were on-going, an operation was planned to capture the entire area south of the Litany River. The operation was approved by the Israeli government because they thought it would give both military and political flexibility. Israeli troops in the area nearly tripled, and on the 12th of August, the operation began, but with a one day duration as the ceasefire took effect on the 13th of August 2006 (Huovinen, 2011, p. 32-33).

4.5 The Failure of the Israeli Doctrine

Before the Second Lebanon War Israel's security situation was like that of the USA with preparations been done for full- spectrum operations including:

- **Low Intensity Conflict (LIC)** mainly focused on the West Bank and Gaza.
- **High Intensity Conflict (HIC)** against contiguous states, like Syria and Lebanon, and “states without common borders” especially Iran.

Accordingly, three group of events affected Israeli perceptions about future warfare prior to the 2006 Second Lebanon War:

- The 1999 war in Kosovo, Operation Enduring Freedom in Afghanistan (OEF-2002) and Operation Iraqi Freedom (OIF-2003) spurred a belief in the Israeli defense Headquarters (HQ) that standoff attacks, mainly by air fire power, was an effective means to affect the will of the adversary and determine conflict outcomes. This approach also seemed to promise lower IDF casualties, less collateral damage and budgetary savings.
- The second al-Aqsa intifada, which began in late 2000, forced the Israeli Army to focus on operations to stop terrorist attacks inside Israel by PLO.
- The USA presence in Iraq following OIF, coupled with low threats from neighbours except Syria, encouraged a belief that Israel was beyond the era of a major war and that the primary role of ground forces was LIC (Johnson, 2010, p. 2).

The findings of the Israeli government’s Winograd Commission, which examined the 2006 Second Lebanon War after its conclusion, showed the problems and chain of command’s “obstacles” that this kind of thinking had caused in some of Israel’s making them to believe that their country had left behind the era of wars and had enough military superiority to deter others from declaring war against her, reminding at the same time to anyone who seemed to be undeterred with sent “messages”. Accordingly, if Israel did not intend to initiate a war, the main challenge of its land forces would be asymmetrical LICs (Johnson, 2010, p. 2).

The mindsets of military and political leaders were fundamentally shaped by this view of Israel’s future security environment, setting actually that their main opponent in the future would be the HW, resulting then in significant cuts in defense spending for ground forces, that also affected training, procurement and logistical readiness, particularly for reserve ground and active heavy units, which all of them had a bad influence upon the effectiveness that gave superiority to the IDF against their numerous neighbouring Arabs The active Israeli Army focused on stopping terrorist attacks, using targeted assassinations and air strikes to “mow the grass,” and raids against high-value targets, all enabled by close coordination with Israeli security services (Mosad). Apparently, they were very successful at LIC in the years before the Second Lebanon War, suppressing the intifada and dramatically lowering Israeli casualties (Johnson, 2010, p. 2).

However, as operations in Lebanon in 2006 showed, the IDF’s almost exclusive focus on LIC resulted in a military that was incapable of joint combined arms fire and maneuver. As operations in Gaza and the West Bank were highly centralized and mainly conducted by small active infantry formations and SOF, the fundamental task was to avoid Israeli military casualties. Thus, the timing of missions became discretionary as the doctrine was “zero casualties to our forces.” The IDF could wait for the best time to strike. Also, heavy units played minor role in these operations. Armored unit training was neglected, because they were deemed largely irrelevant in LIC. In addition to this, training and exercises for division and higher units were infrequent and the IDF posted the best brigade commanders to deal with LIC threats. Finally, IAF tactical air control capabilities were pulled out of ground brigades, a crucial point bearing in mind that IAF owns almost all fixed-wing and rotary-wing aircraft when the Israeli Army has only small UAVs (Johnson, 2010, p. 3).

During the Second War of Lebanon, the IDF faced terrain and enemy conditions for which they were not prepared. An Israeli journalist, underlined that in the years preceding the operation in Lebanon none of the Israeli units were required to counter an enemy force of a size larger than an unskilled infantry squad (Johnson, 2010, p. 3).

Hezbollah, although not being so powerful in military terms, was trained and organized into small units, armed with sophisticated weapons, including anti-tank guided missiles, Rocket Propeller Grenades (RPGs) (including RPG-29s), rockets, mortars, mines, IEDs, and Man Portable Air Defence Systems (MANPADS). It also occupied prepared defensive positions in Lebanon’s difficult hilly terrain and urban areas. So, one of the major deficiencies of the Israeli Army was that, as it was highly conditioned by its LIC experience, was opposed against an enemy force that presented a high-intensity challenge that required joint combined arms fire and maneuver and a combat mindset different from that of PLO, even though Hezbollah did not have large formations. An IDF Israeli observer noted that as before the Second Lebanese war most of the regular IDF were engaged in combating PLO, when they were transferred to Lebanon, they were unfit to conduct combined force battles integrating infantry, armored, engineering, artillery forces e.t.c.

(Johnson, 2010, p. 3-4).

This fact was fundamentally apparent with field artillery and air. Hezbollah was a disciplined and trained adversary, operating in cohesive small units and occupying good terrain, having also standoff ammunition (AntiTank Guided Missiles-ATGMs, mortars and rockets) capability. Thus, defeating Hezbollah required joint combined arms fire and maneuver, something the IDF was largely incapable of executing in 2006. Fire suppresses enables ground maneuvering forces to fight close with him. Fire also isolates the enemy, shutting off lines of supply and communication, limiting also his ability to mass. Thus, hybrid opponents like Hezbollah demand integrated joint air ground and ISR capabilities that are similar to those used against conventional adversaries, but at a reduced scale. Finally, the IDF's highly centralized C2 system, which had been effective in confronting the intifada, proved problematic against Hezbollah. In conclusion, IDF was not prepared for ground operations when standoff strikes did not force Hezbollah to meet Israeli demands (Johnson, 2010, p. 2).

After the 2006 Second Lebanon War, the IDF underwent intense internal and external renewal. Regarding the military reformal, the Winograd Commission stated that the Chief of Staff did not alert the political echelon to the serious shortcomings in the preparedness and the fitness of the armed forces for an extensive ground operation, if that was inevitable, and he did not clarify that from the analysis done about the theater of operations that there was a high probability that a military strike against Hezbollah would make ground operations necessary (Johnson, 2010, p. 4).

The IDF set about correcting the deficiencies identified in the Second Lebanon War, particularly in its ground forces. Several generals resigned or were fired, including the chief of staff, Lieutenant General Dan Halutz. Additional resources were invested in training and equipping, for both reserve and active forces. Most important, the IDF shifted its training focus from LIC to HIC and a "back to basics" approach that emphasized joint combined arms fire and maneuver training. The IDF also rethought the role of heavy forces, concluding that tanks can provide better protection to their crew than in the past if they are correctly deployed and therefore IDF requires an annual supply of dozens of advanced tanks in order to replace the older and more vulnerable versions (Johnson, 2010, p. 4).

Thus, production of the Merkava IV tank resumed, and the IDF began work on fielding the Namer, a heavy Infantry Fighting Vehicle (IFV) based on the Merkava class, to replace less capable systems like the Achzarit IFV, based on a T-55 tank class, and M-113 armored personnel carriers. Finally, procedures to integrate artillery and air fires into maneuver brigades were adopted and practiced and air controllers were again assigned to maneuver brigades (Johnson, 2010, p. 4-5).

4.6 Conclusion

Looking at the outcome of the Second Lebanon War, it is obvious that Hezbollah emerged as the one having better reached and succeeded its' set of strategic goals for the war than Israel, which actually were (Huovinen, 2011, p. 33):

- Survive to an Israeli-driven escalation.
- Inflict maximum casualties in forward area of operations.
- Win limited war of attrition.
- Demonstrate the ability to strike into Israel with short and long range weapons.
- Dominate media battle (IW).
- Enhance post-war status in Lebanon and Islamic world.
- Emerge with political leadership.
- Prevent from being disarmed after the war so it would continue its HW action in the future.

Israel could not restore credibility of deterrence, but the effect was rather the opposite. Kober points out serious weaknesses of IDF were exposed (Kober, 2008, p. 8-9):

- A late perception of that it was war.
- Adherence to post-heroic warfare under circumstances that rather required a different approach.
- The erosion of the IDF's fighting standards due to policing missions.
- The artificial RMA – inspired concepts.
- The adoption of the notion of controlling instead of capturing territory.
- A centralized logistic system.

- Poor generalship.
- A hesitant and inexperienced political leadership and IDF dominance in decisions on military matters.

On the other side, Lebanon was not forced to act as a credible state to end the Hezbollah's "state-with-in-state" status, but to ask the international community for support against the Israeli aggression towards Lebanon (Huovinen, 2011, p. 33).

Moreover, Hezbollah was unable to inflict real heavy casualties to IDF or Israel in general, but the damages caused were higher than expected, and as Israel has a democratic elected government, casualties is always a problem with great psychological impact. The long range missile weapon systems were used in the beginning of the war, but were quickly taken out by the IAF. Yet the continuous use of short range rockets and the use of UAV demonstrated adequately the Hezbollah striking capability beyond close range. As a result of the ceasefire Hezbollah was not disarmed nor was incapacitated, and so it could continue rebuilding its' lost capabilities and playing an important role on Lebanese politics (Huovinen, 2011, p. 33-34).

The reasons for Hezbollah's achievements are many. It can be said that Israel underestimated the new capabilities of Hezbollah, both politically and militarily and at the same time overestimated its own capability to win the war by waging only an air campaign without the use of extensive ground operating brigades. However, the biggest failure of Israel was that it escalated the retaliatory operation into a war before the Israeli government had decided whether to conduct a short and powerful hit against Hezbollah or to bring about a significant change in Southern Lebanon with a large ground operation, while at the same time the Israeli government had not decided in a back up/exit strategy if its' planning did not come out as it wanted to be (Huovinen, 2011, p. 33).

Not only did Hezbollah possess weapons usually associated with national armies, but it used them with considerable precision and skill. With modern weapons and advanced guerrilla tactics included and by using civilian targets as shields for operative troops was something IDF was not prepared to face, endorsing that way the sayings of Sayyid Hassan Nasrallah, the Secretary General of Hezbollah, that Hezbollah is not a regular army and will not fight like a regular army (Huovinen, 2011, p. 34).

The C2 system of Hezbollah was decentralized and responsibilities were distributed to smaller cells, giving the organization flexibility and strength to carry on fighting despite the fact that any of these independent cells were incapacitated. During the years before the war, Hezbollah had plenty of time to build its defensive positions in Southern Lebanon according to their estimates of possible battle spaces and prepare for the eventually inevitable armed conflict against Israel, shaping its own doctrine in every single level of its echelon. Along with a decentralized logistics system, the small cells had well planned resources available for them and gave them logistical independence from the upper echelons (Huovinen, 2011, p. 34).

The Second Lebanon War demonstrated also the capability of a nonstate actor like Hezbollah to wage war successfully against an army like the IDF by studying and deconstructing the vulnerabilities of Western style military and formulate appropriate countermeasures, putting together elements of war to HW tactics and used them as force multipliers to its advantage, including advanced weapons, well trained troops in irregular warfare, use of media to distribute as self-profitable information, disregard of the lives of own and civilian casualties, the inclusion of a strong religious background and the knowledge of the opponent with the inclusion of political and military capabilities and restrictions, and especially the opponent's moral limitations. Hoffman describes these features as a *"blend of lethality of state conflict with the fanatical and protracted fervor of irregular warfare."* (Hoffman, 2007, as cited in Huovinen, 2011, p. 35).

The Second Lebanon War served as a good example, how to fight and be successful against a western military driven force and the lessons concluded have been learned and studied by other organizations like Hezbollah. These are the types of conflict western militaries will be faced with in the future (Huovinen, 2011, p. 35).

However, some analysts in Israel have all too quickly dismissed the unique character of Hezbollah. These analysts blithely focus inward on the failings of the political and military leadership. This is a fatal disease for military planners, one that can only benefit future Hezbollahs. As Winston Churchill perfectly once stated that it is sometimes necessary to take the enemy into account no matter how much absorbed a commander may be in the elaboration of his own thoughts (Hoffman, 2009, p. 38).

Russell Glenn, a retired U.S. Army officer now with RAND, conducted an objective evaluation and concluded that the second Lebanon conflict was inherently **heterogeneous** and that attempts to focus on purely conventional solutions were futile as 21st century conflict has up to nowadays been typified by HW (Hoffman, 2009, p. 38).

In conclusion, Hezbollah will continue to be **a strategic irritant and the main innovator of hybrid ways and means**. Already demonstrated in 2006 Second Lebanon War, Hezbollah continually seeks innovative ways to accomplish its objectives. Through a composite mix of symmetric and asymmetric capabilities fused at the operational level, Hezbollah in many ways is a fortified conventional army and guerilla force at the same time, functioning distributed operations and rapid transition of force mix which demonstrates a potent lethal combination which also conducted Signals Intelligence (SIGINT) operations against IDF communications. Through a mixture of conventional, irregular, and terrorist tactics Hezbollah inflicted more Israeli casualties per Arab fighter in 2006 than did any of Israel's state opponents in the 1956, 1967, 1973, or 1982 Arab-Israeli interstate wars (Burbridge, 2013, p. 14).

Hezbollah political and military sophistication surprised Israel by exploiting their military actions and Israeli military errors through the power of information. Hezbollah used the internet and sympathetic international media extensively to expand the impact of their military efforts to audiences regionally and internationally. Further, Hezbollah succeeded in blaming Israeli forces for collateral damage against Lebanese civilians to draw international criticism against the Israeli government. While those in many other countries had thought Israel was justified at the incursion's start, audiences opinion was transformed as they saw images of Lebanese civilian casualties (both fabricated and real) (Burbridge, 2013, p. 14).

Hezbollah's IW operations were compounded by Hezbollah's diplomatic efforts, so that the Israeli local and international media and diplomatic effort was outclassed (Burbridge, 2013, p. 14).

The result of Hezbollah's military, informational and diplomatic efforts gained moral legitimacy as Hezbollah was declared the defender of the Lebanese people. The totality of Hezbollah efforts allowed their narrative to defeat the Israeli one. That perceptual victory became reality, allowing Hezbollah to maintain the status quo in spite of the damage they took on the battlefield *(*Burbridge, 2013, p. 14).

CHAPTER 5

Strategy against the Hybrid Threats

5.1 Introduction

In the previous chapters of the present dissertation, it has been crystal clear through the analysis of case studies that hybrid threats are a continuous enemy of sovereign democratic states and its civilians, which have to resist against them. Moreover, in this chapter will be described the actions and the legit documentation that EU and NATO have issued for the abovementioned reasons. But first, it is necessary to detect and recognize the threat. So, the following phases are recognized in the warning process:

- Direction of the warning efforts.
- Collecting the information.
- Analysis of the threats.
- Communicating the warning analysis (Rietjens, 2020, p.3 ; Andersson & Tardy, 2015).

Phase I: In line with the traditional view on warning, policymakers or military commanders provide direction for the warning process by stating their needs (**information requirements)**. However, for hybrid threats, such initial requirements are often impossible to get defined. Compounding this problem is the multitude of participating actors in the warning process and at the same time the lack of ownership of this process. While traditional threats had one specific organization that provided guidance to direct the warning process, this is less so in hybrid conflicts because of their nature and their aggression against both civilian and military targets in a 24/7 basis. Constantly changing actors bring relevant resources to the foreground, questionable in terms of funding, coordination and human resources, calling thus for an alternative way of dealing with the direction of the warning process. The following design principles assist in the development of a self-organized warning system (Rietjens, 2020, p.3):

- The first principle of self-organization is “the importance of redundancy”. Organizations need to invest in slack information processing capabilities and skillsets to decrease responsive dependency on the actions of a single local actor.
- The second principle is to obey Ashby’s law of “requisite variety”, which means that the internal diversity must match the variety and complexity of its environment.
- The third principle is labeled as “minimum specs”, which implies that the leadership must only define the essentials and offer enough freedom for distributed action to officers.
- The fourth principle is “learning to learn”. This principle emphasizes that in order to self-organize, members must possess a mindset of constant feedback learning, but must also be granted the freedom to challenge existing norms, rules and procedures mainly in the intelligence services (Rietjens, 2020, p.3-4).

Phase II: Indicators are at the heart of the warning data collection process, providing a systematic framework for monitoring the situation and creating an alert. They are important in order to reduce the complexity of every single situation and transform them to manageable concrete features, assigned with useful issues whereas any change in them could be easily noticed(Odote, 2016).

Warning academics identify several requirements for indicators, the most prominent being predictive, diagnostic, unambiguous and collectible. Here, a great diversity of instruments, both military and non-military, as well as threat actors need to be understood and monitored to provide adequate warning. This challenge is enormous and demands bridging the gap between deductive and inductive methods that use qualitative as well as quantitative data. When applying deductive methods, indicators are formulated upfront and based on general ideas or insights. Apart from defining indicators that are based on established knowledge, it is important to apply inductive methods that start with observations and move backwards to generalizations. In addition, there is a growing consensus that warning methods need to integrate quantitative as well as qualitative data. Most warning methods seem to prefer quantitative data and as long as these data are reliable, valid, timely, and adequately analyzed, these methods are indispensable. (Rietjens, 2020, p. 4).

Phase III: While many policymakers like to refer to "connecting the dots" to derive accurate images of forthcoming events, this picture is highly inaccurate and unhelpful. In the case of hybrid threats, the dots are missing because they are usually impossible to be understood due to some kind of encryption. So, analysts have started to borrow sophisticated methods from other domains as wide and varied as weather prediction, ecology, business management, and consumer behavior forecasting. Part of this methodology is the ability to take local knowledge or the views of people on the ground into account, so that one can bridge the gap between what analysts with their computer models and their internet searches collect as information and what is happening on the ground by using NGOs, embassies, e.t.c. (in vivo, in vitro and in situ analysis). Another point that has to been carefully examined is incorrect and misleading information, delivered either intentionally (disinformation) or unintentionally (misinformation) (Rietjens, 2020, p. 5).

Phase IV: Warning is the timely response so that harm is prevented or at least reduced by appropriate action. Effectively communicating the warning to decision makers or to the population is therefore crucially significant, including characteristics such as source credibility, message content and mode of communication. The extent to which the warning message finally influences actual decision making process and triggers a response depends on many other factors, with most important the perception of the receiver (Rietjens, 2020, p. 6).

5.2 European Union's Actions

5.2.1 Stakeholders

A]European Commission Directorate General (DG) for Internal Market, Industry, Entrepreneurship and Small and Medium Sized Enterprises (SMEs): The mission of DG Internal Market, Industry, Entrepreneurship and SMEs is to develop a deeper and fairer internal market and help European enterprises, manufactures and service industries to be globally competitive, innovative and sustainable by creating more jobs, growth and value for all. The DG is a major contributor to four of the Commission's priorities (European

Commission, 2022a):

- A new boost for jobs, growth and investment.
- A deeper and fairer internal market with a strengthened industrial base.
- A connected digital single market.
- A resilient energy union with a forward looking climate change policy.

According to its strategic plan 2016-2020, the DG is working together with the EEAS to counter hybrid threats.

B]European Commission Directorate-General for Migration and Home Affairs: DG for Migration and Home Affairs creates policies that aim to ensure that all activities necessary and beneficial to the economic, cultural and social growth of the EU can develop in a stable, lawful and secure environment. It aims to develop a balanced and comprehensive EU migration policy, based on solidarity and responsibility, building a safer Europe by fighting terrorism and organized crime, by promoting police cooperation and by preparing to respond swiftly to emerging crises. DG Migration and Home Affairs, together with the JRC, develops tools and vulnerability indicators to address hybrid threats to critical infrastructures (European Commission, 2022b).

C]European Commission Directorate-General Joint Research Centre (JRC) is the European Commission's science and knowledge service. It has solid research and policy support experience as well as broad networks with academia, industry, Member States and city authorities (European Commission, 2022c).

D]European External Action Service (EEAS): The EEAS is the EU's diplomatic service, which works closely with the foreign and defense ministries of the EU Member States and with EU institutions. It also has a strong working relationship with the UN and other international organizations. It helps the High Representative/Vice President (HR/VP) to implement the EU's Common Foreign and Security Policy (CFSP) (European Union, 2022a).

E]EU Hybrid Fusion Cell: It was established in 2016, within the existing EU Intelligence and Situation Centre, aiming to provide all-source analysis on hybrid threats. As envisaged in the joint framework on countering hybrid threats, it receives, analysis and shares classified and open-source information specifically relating to indicators and warnings concerning hybrid threats. In liaison with similar bodies at EU and national levels, the Fusion Cell deals with external aspects of hybrid threats affecting the EU and its neighbourhood, rapidly analysing relevant incidents and informing the EU's strategic decision-making processes, by providing also inputs into the security risk assessments carried out at EU level. Member States are expected to establish national Points Of Contact (POC) connected to the EU Hybrid Fusion Cell. Communication task forces for the EU's eastern and southern neighbourhoods have been established to counter widespread disinformation campaigns and systematic diffusion of fake news. The guidelines issued on the basis of the Council conclusions of March 2015 provided a mandate for establishing the EEAS East Strategic Communication (StratCom) Task Force. Additionally, in 2017, the EEAS decided to set up two forces, the EEAS StratCom Western Balkans Task Force and the EEAS StratCom South Task Force. The East StratCom Task Force develops communication products and campaigns focused on better explaining EU policies in the Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine). The task force reports on and analysis of disinformation trends, explain and correct disinformation narratives, raising also awareness of disinformation. It additionally works with the EU institutions, EU delegations in the Eastern Partnership countries, Member States and a wide range of other partners, both governmental and non-governmental, within the EU, in the eastern neighborhood, and beyond. This international cooperation aims to share best practices in strategic communications and provide access to objective information, as well as ensuring support for independent media in the region (Kert-Saint Aubyn, M., 2022).

F]European Defence Agency (EDA): This is an intergovernmental agency of the Council of the European Union, to which it reports and from which it receives guidelines, having three main tasks:

- Supporting the development of defense capabilities and military cooperation among the EU Member States.
- Stimulating defense research and technology and strengthening the European defense industry.
- Acting as a military interface to EU policies.

One of the domains in which the EDA is active is cyber and hybrid warfare. This work comprises several projects on topics such as cyberdefence, radiofrequency sensor technologies, information, optronics, governmental satellite communications, communications and information systems, persistent surveillance long-term analysis and hybrid warfare. In 2016, the EDA organized the Hybrid Threats Table Top Exercise, with the participation of DG Internal Market, Industry, Entrepreneurship and SMEs, DG Energy, DG Mobility and Transport, DG Migration and Home Affairs, Europol and many others, as well as observers from NATO. The objective of the exercise was to identify and analyze the implications of hybrid threats for European military capability development. The EDA is currently managing the Consultation Forum for Sustainable Energy in the Defence and Security Sector, a European Commission initiative aimed at bringing together specialists from the defense and energy sectors to share data and best practices (European Union, 2022b).

G]European Union Agency for Law Enforcement Cooperation (Europol): Europol is the EU’s law enforcement agency. It supports the EU Member States in their fight against terrorism, cybercrime and other serious and organized forms of crime. It also works with many non-EU partner states and international organizations. The EU Internet Referral Unit (IRU) was set up by the Justice and Home Affairs Council of the EU and is built upon Europol’s Check the-Web service. Its main role is to anticipate and pre-empt terrorist abuse of online tools, as well as to play a proactive advisory role in relation to EU Member States and the private sector in this regard. Additionally focuses on:

- Supporting the competent EU authorities by providing strategic and operational analysis.
- Flagging terrorist and violent extremist online content and sharing it with relevant partners.
- Detecting and requesting the removal of internet content used by smuggling networks to attract migrants and refugees.
- Swiftly carrying out and supporting the referral process, in close cooperation with the industry (European Union, 2022c).

The EU IRU’s tactical approach to the abovementioned is targeted. The procedure aims to focus on propaganda linked to a high-profile event (e.g. the Paris attacks, the Brussels attack) and relayed by high profile accounts. The primary objective is to be effective during the “viral” phase of the propaganda. The secondary objective is to gather information to better understand the tactics and modus operandi of the main online propagandists in order to improve the disruption mechanism (Europol, 2022).

5.2.2 Measures

The first line of EU response to hybrid threats proposed by the EEAS involves **improving awareness** by mainly establishing a clear understanding of what exactly hybrid threats are, i.e. how they differ from non-hybrid ones. For example, a terrorist group which mainly plants bombs or makes use of suicide bombers does not, in and by itself, constitute a hybrid threat. It is only if and when such an outfit combines tactics, such as, the launching of military campaigns, systematically spreading disinformation or running criminal activities that the threat mutates into a hybrid one. Terrorism, cybercrime, trafficking and extortion are not per se hybrid in nature, but they may become so depending on how they are pursued using multiple tactics simultaneously (Andersson & Tardy, 2015, p. 1).

It may even be the case that some threats originated from a particular organization or state are hybrid while others issued by the same agent are not, posing that the threats must constantly be reviewed in light of state of the art developments (Andersson & Tardy, 2015, p. 2).

Additionally, the multi-layered and multi-faced nature of hybrid threats calls for an equally multi-task response, with a view to “building resilience” and “responding to attacks” from the member states as a whole inside the Union. Here, the EU’s “comprehensive approach” comes to the fore, as it provides an appropriate framework for policy response and an added value for the Union (Andersson & Tardy, 2015, p. 2).

In an EU context most important is the mix of external and internal security policies and instruments which is likely to provide the most appropriate response. Consequently, the comprehensive approach, insofar as it is mainly about the EU’s external action, would need to be broadened so as to include elements of internal security, such as:

- Member states’ instruments and activities.
- EU internal security instruments, i.e. freedom, security and justice tools, and those of the European Commission.
- EU external security instruments (including CSDP operations and missions), and

NATO activities (Andersson & Tardy, 2015, p. 2).

An interesting example which requires such an approach is the handling of “foreign fighters”, i.e. individuals who spend time in war-torn or lawless areas before returning and becoming potential threats to their own country (or others). For any EU member state dealing with this issue, the response will combine exclusively national policies, cooperation at EU level on law enforcement, border controls and intelligence sharing, as well as possible EU initiatives aimed at capacity building in third countries or disrupting hostile activities wherever they take place, such as the NATO acts. This makes the coordination of various lines of response more vital and comprehensive (Andersson & Tardy, 2015, p. 3).

In the meantime, the confusion intentionally created by hybrid tactics is likely to further complicate the ability of EU countries and institutions to craft a truly coherent and comprehensive response. In order to respond effectively, the EU not only has to develop a cyber-security strategy, a maritime strategy or a broader ‘global’ strategy but also has to learn how to synchronize all these aspects (Andersson & Tardy, 2015, p. 3).

The first and arguably main line of response will likely lie with the member states. The EU, therefore, needs to demonstrate its added value when it comes to improving awareness, building resilience, and responding to attacks. In this effort, the Commission will have a key role. In any case, both the EU and its member states will have to develop generic responses to those very different types of threats. The Ukraine crisis in the spring of 2014, as it was analyzed in Chapter 3, allowed for a conceptual but somehow artificial grouping of the two threats under a common hybrid label (Andersson & Tardy, 2015, p. 3).

Indeed, this has been the case to date at all the three levels of awareness, resilience and response. Ultimately, the very heterogeneity of hybrid threats may cast doubts on the utility of developing a general, catch-all strategy to counter them. So, the dangers of hybrid operations against the Union and its partners are real (Andersson & Tardy, 2015, p. 3).

On the other side, it is imperative that a military response by the EU should have the capability to (Andersson & Tardy, 2015, p. 3-4):

- Act as a deterrent: No EU member state is strong enough to withstand a large-scale for instance Russian operation on its own.
- Quickly react even without outside help: If a group of “little green men” lacking

visible insignias were to occupy a village in an EU or NATO member state bordering Russia, that country's military and security forces must have the capability to rapidly respond on their own.

- Rapidly deploy to another EU or NATO member state in case of request and need: While the US keeps a rotating force of 150 troops in each of the Baltic states and Poland since April 2014 (occasionally joined by similar-sized units from other NATO allies), more troops would be needed in the event of a crisis.
- Effectively support civilian authorities and police: In cases of large-scale violent riots or acts of domestic terrorism associated with hybrid operations, police forces may be overwhelmed, contributing to the sense of confusion and hopelessness. In some countries, the police have the possibility to draw on military assets and personnel to act under civilian command.

In all these cases, operational readiness will be important. In particular, SOF could play important roles in quickly establishing a military presence on the ground and providing intelligence in contested territories. Other important military assets in countering hybrid operations are airborne surveillance and remote sensor capabilities to provide necessary early warning and intelligence (Andersson & Tardy, 2015, p. 4).

Another central aspect is that of the strategic communications, enforced by defensive and offensive psychological operations ("psy-ops"). Once a hybrid operation is successfully defeated, military capabilities may also be important for post-conflict peace-stabilisation missions. Such missions could include tasks like policing semi-permissive environments and would require close cooperation with civilian actors.

Really interesting about potential hybrid threats are the following statistics:

- Connected devices forecast to rise to 25 billion by 2025, a quarter of these in Europe.
- Changes in working patterns accelerated by the COVID-19 pandemic – 40% of EU workers switched to telework in early 2020.
- 2/5 of EU users have experienced security-related problems.
- 1/8 of businesses have been affected by cyber attacks.
- The annual cost of cybercrime to the global economy is estimated at €5.5 trillion by the end of 2020, double compared to 2015.

- EU funding in the 2021-2027 Multiannual Financial Framework could amount to €2 billion overall plus Member States and industry investment.
- EU investments in digital projects should amount to at least 20% - equivalent to €134.5 billion - of the €672.5 billion Recovery and Resilience Facility (European Commission, 2020a).

In the institution's level EU has reached a political agreement, subject to formal approval by the European Parliament and the Council of the EU, on the **Cybersecurity Competence Centre and Network**, an initiative that aims to improve and strengthen technology and industrial cybersecurity capacities of the EU and help create a safe online environment. The Cybersecurity Competence Centre, which is located in Bucharest, and the Network of National Coordination Centers aim at strengthening European cybersecurity capacities, shielding the economy and society from cyber attacks, maintaining and promoting research excellence and reinforcing the competitiveness of the Union's industry in this field. The Centre and the Network will pool resources from the EU, its Member States and the industry to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy. The Cybersecurity Competence Centre and Network will help the Union and Member States to take a proactive, longer-term and strategic perspective to cybersecurity research, development, and industrial policy, by enhancing their technological sovereignty through large-scale Cybersecurity projects in areas such as Cyber Threat Intelligence, Cyber secured hardware and operating systems and security certification (ECCC, 2022).

As a key component of Shaping Europe's Digital Future, the Recovery Plan for Europe and the EU Security Union Strategy will bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The new Cybersecurity Strategy also allows the EU to step up leadership on international norms and standards in cyberspace, and to strengthen cooperation with partners around the world to promote a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values. Furthermore, the Commission is making proposals to address both cyber and physical resilience of critical entities and networks: A Directive on measures for high common level of cybersecurity across the Union (*revised NIS Directive or "NIS 2"*), and a new Directive on the resilience of critical entities.

(National Security Authority, 2020).

It contains concrete proposals for regulatory, investment and policy initiatives, in three areas of EU action (European Commission, 2020b):

- Resilience, technological sovereignty and leadership: Commission proposes to reform the rules on the security of network and information systems, under a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2'), in order to increase the level of cyber resilience of critical public and private sectors: hospitals, energy grids, railways, but also data centres, public administrations, research labs e.t.c. .
- The Commission also proposes to launch a network of Security Operations Centres across the EU, powered by Artificial Intelligence (AI), which will constitute a real "cybersecurity shield" for the EU, able to detect signs of a cyberattack early enough and to enable proactive action, before damage occurs. Additional measures will include dedicated support to SMEs, under the Digital Innovation Hubs, as well as increased efforts to upskill the workforce, attract and retain the best cybersecurity talent and invest in research and innovation that is open, competitive and based on excellence. Building operational capacity to prevent, deter and respond the Commission is preparing, along with the Member States, a new Joint Cyber Unit. In addition to this, the High Representative puts forward proposals to strengthen the EU Cyber Diplomacy Toolbox to prevent, discourage, deter and respond effectively against malicious cyber activities.
- Advancing a global and open cyberspace through increased cooperation The EU will step up work with international partners to strengthen the rules-based global order, promote international security and stability in cyberspace, and protect human rights and fundamental freedoms online. It will advance international norms and standards that reflect these EU core values, by working with its international partners in the UN and other relevant fora. The EU will also form an EU Cyber Diplomacy Network around the world to promote its vision of cyberspace.
- Cyber and physical resilience of network, information systems and critical entities. Existing EU-level measures aimed at protecting key services and infrastructures from both cyber and physical risks need to be updated. Physical risks have become more complex since the adoption of the 2008 EU rules on critical infrastructure,

which currently only cover the energy and transport sectors.

- NIS 2 strengthens security requirements imposed on the companies, addresses security of supply chains and supplier relationships, streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States. The NIS 2 proposal will help increase information sharing and cooperation on cyber crisis management at national and EU level. The proposed Critical Entities Resilience (CER) Directive expands both the scope and depth of the 2008 European Critical Infrastructure directive. Ten sectors are now covered: **energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space.** Under the proposed directive, Member States would each adopt a national strategy for ensuring the resilience of critical entities and carry out regular risk assessments. These assessments would also help identify a smaller subset of critical entities that would be subject to obligations intended to enhance their resilience in the face of non-cyber risks, including entity level risk assessments, taking technical and organisational measures, and incident notification. The Commission, in turn, would provide complementary support to Member States and critical entities, for instance by developing a Union-level overview of cross-border and cross-sectoral risks, best practice, methodologies, cross-border training activities and exercises to test the resilience of critical entities.
- Securing the next generation of networks: 5G and beyond. The new Cybersecurity Strategy proposes to integrate cybersecurity into every element of the supply chain and bring further together EU's activities and resources across the four communities of cybersecurity – internal market, law enforcement, diplomacy and defence. It builds on the EU' Shaping Europe's Digital Future and the EU Security Union Strategy, leaning on a number of legislative acts, actions and initiatives the EU has implemented to strengthen cybersecurity capacities and ensure a more cyber-resilient Europe. This includes the Cybersecurity strategy of 2013, reviewed in 2017, and the Commission's European Agenda on Security 2015-2020. The first EU-wide law on cybersecurity, the NIS Directive, that came into force in 2016 helped to achieve a common high level of security of network and information systems across the EU. As part of its key policy objective to make Europe fit for the

digital age, the Commission announced the revision of the NIS Directive in February this year. The EU Cybersecurity Act that is in force since 2019 equipped Europe with a framework of cybersecurity certification of products, services and processes and reinforced the mandate of the EU Agency for Cybersecurity (ENISA). As regards Cybersecurity of 5G networks, Member States, with the support of the Commission and ENISA have established, with the EU 5G Toolbox adopted in January 2020, a comprehensive and objective risk-based approach.

- The EU has supported third countries in increasing their cyber resilience and ability to tackle cybercrime, and has used its 2017 EU cyber diplomacy toolbox to further contribute to international security and stability in cyberspace, including by applying for the first time its 2019 cyber sanctions regime and listing 8 individuals and 4 entities and bodies. The EU has made significant progress also on cyber defense cooperation, including as regards cyber defence capabilities, notably in the framework of its Cyber Defence Policy Framework (CDPF), as well as in the context of the Permanent Structured Cooperation (PESCO) and the work of the European Defence Agency. Cybersecurity is also a priority reflected in the EU's next long-term budget (2021-2027). Under the Digital Europe Programme the EU will support cybersecurity research, innovation and infrastructure, cyber defence, and the EU's cybersecurity industry. In addition, in its response to the Coronavirus crisis, which saw increased cyberattacks during the lockdown, additional investments in cybersecurity are ensured under the Recovery Plan for Europe. The EU has long recognised the need to ensure the resilience of critical infrastructures providing services which are essential for the smooth running of the internal market and the lives and livelihoods of European citizens. For this reason, the EU established the European Programme for Critical Infrastructure Protection (EPCIP) in 2006 and adopted the European Critical Infrastructure (ECI) Directive in 2008, which applies to the energy and transport sectors. (European Commission, 2020b).

5.2.3 Threats of disinformation

Disinformation is an evolving threat which requires continuous efforts to address the relevant actors, vectors, tools, methods, prioritised targets and impact. Some forms, especially state-driven disinformation, are analyzed by the EU Hybrid Fusion Cell, in cooperation with the Strategic Communication Task Forces of the EEAS and with the support of Member States' services (European Commission, 2018, p. 3).

The actors behind disinformation may be internal, within Member States, or external, including state and non-state actors. According to reports, more than 30 countries are using disinformation and influencing activities in different forms, including in their own countries. The use of disinformation by actors within Member States is an increasing source of concern across the EU. Cases of disinformation driven by non-state actors have also been reported, for example related to Covid-19 vaccination. As regards external actors, the evidence is strong in the case of the Russian Federation. However, other third countries also deploy disinformation strategies, learning from the methods of the Russian Federation (European Commission, 2018, p. 4).

According to the EU Hybrid Fusion Cell, disinformation by the Russian Federation poses the greatest threat to the EU. It is systematic, well-resourced, and on a different scale to other countries as it was described in Chapter 3. In terms of coordination, levels of targeting and strategic implications, Russia's disinformation constitutes part of a wider hybrid threat that uses a number of tools, levels, and also non-state actors (European Commission, 2018, p. 4).

On a parallel line, social media have become important means of spreading disinformation, including as well the delivery of disinformation content to specific users, who are identified by the unauthorized access and use of personal data, with the ultimate goal of influencing the election results. Recent evidence shows that private messaging services are increasingly used to spread disinformation. Techniques include video manipulation (*deep-fakes*) and falsification of official documents, the use of internet automated software (*bots*) to spread and amplify divisive content and debates on social media, troll attacks on social media profiles and information theft. At the same time, more traditional methods such as television, newspapers, websites and chain emails continue to play an important role in many regions. The tools and techniques used are changing fast so the response needs to evolve just as rapidly (European Commission, 2018, p. 4).

Consequently, the EEAS has set up specific strategic communication task forces consisting of experts with relevant language and knowledge skills in order to develop response strategies. (European Commission, 2018, p. 4).

Based on the Action Plan on Strategic Communication, adopted on the 22nd of June 2015, the mandate of the East Strategic Communication Task Force comprises three strands of action (European Commission, 2018, p. 4):

- Effective communication and promotion of Union policies towards the Eastern Neighbourhood.
- Strengthening the overall media environment in the Eastern Neighbourhood and in Member States, including support for media freedom and strengthening independent media.
- Improved Union capacity to forecast, address and respond to disinformation activities by the Russian Federation. In response to the Council conclusions in December 2015 and June 2017, the EEAS set up two additional task forces: The Western Balkans Task Force 24 for the corresponding region and the Task Force South 25 for the countries in the Middle East, Northern Africa and the Gulf region.

Since it was established, the East Strategic Communication Task Force has effectively communicated on the policies of the Union in the Union's Eastern neighbourhood mainly through a campaigns-led approach. In addition, the East Strategic Communication Task Force has catalogued, analyzed and put the spotlight on over 4,500 examples of disinformation by the Russian Federation (European Commission, 2018, p. 5).

Therefore, addressing disinformation requires political determination and unified action, mobilising all parts and security services of governments. This should be done in close cooperation with like-minded partners across the globe, as long as requiring close cooperation between Union institutions, Member States, civil society and the private sector, especially online platforms. Finally, the coordinated response to disinformation presented in the abovementioned Action Plan is based on four pillars (European Commission, 2018, p. 5):

- Improving the capabilities of Union institutions to detect, analyse and expose disinformation.
- Strengthening coordinated and joint responses to disinformation.
- Mobilising private sector to tackle disinformation.
- Raising awareness and improving societal resilience.

5.3 NATO's Actions

The NATO strategy on countering hybrid threats is structured along the scheme prepare—deter—defend. Enhanced intelligence and surveillance is the key aspect of NATO's response to hybrid threats, while it also constitutes a challenge when it comes to indications for early warning. Cooperation with the EU, which looks at civil society much more closely than NATO, could increase the ability to capture early signs substantially. The implementation plan focuses on "prepare," which is on how to organize NATO Headquarters and coordinate actions with member states and the EU in order to improve the ability to identify, recognize and attribute hybrid attacks quickly, because as it is undoubtedly recognized, in order to be more effective in countering hybrid threats, NATO is committed to working even more closely with the EU. One important finding, and challenge, in the process of addressing hybrid threats within NATO has been that a lot of actions do not fall within the responsibility of the Alliance, but on the member states themselves (Wieslander, 2016, p. 3)

So NATO has set seven baseline requirements to be assessed:

- Assured continuity of government and critical government services.
- Resilient energy supplies.
- Ability to deal effectively with the uncontrolled movement of people.
- Resilient food and water resources.
- Ability to deal with mass casualties.
- Resilient communications systems.
- Resilient transportation systems (Wolf-Diether, 2019 ; Wieslander, 2016, p. 4)

In order to assist allies in meeting those requirements, NATO has agreed to create resilience advisory support teams, as recommended by Hans Binnendijk, Daniel Hamilton and Frank Kramer, to offer expertise, a form of internal consulting, on areas such as cyber attack response, civil-military planning and coordination, protection of critical infrastructure, and so forth. A NATO hybrid cell is expected to cooperate with the EU Hybrid Fusion Cell through direct liaison, as well as regular sharing of analyses and lessons identified. Closely linked to countering hybrid threats are NATO's Centers of Excellence (COEs) on many subjects, such as Energy Security in Vilnius, Strategic Communication in

Riga and Cyber Defence in Tallinn. The COEs assist in doctrine development, identify lessons learned, improve interoperability and capabilities, test and validate concepts through experimentation (Wieslander, 2016, p. 4).

Hybrid Threats were defined in 2011 by NATO as multimodal, low intensity, kinetic as well as non-kinetic threats to international peace and security, including asymmetric conflicts, global terrorism, piracy, transnational organized crime, demographic challenges, resources security, retrenchment from globalization, and the proliferation of weapons of mass destruction. Accordingly, NATO's Allied Command Transformation (ACT), supported by the US Joint Forces Command Joint Irregular Warfare Centre and the U.S. National Defense University (NDU), conducted specialized research into "Assessing Emerging Security Challenges in the Globalized Environment (Countering Hybrid Threats) Experiment". Its' findings were in essence that hybrid threats faced by NATO and its non-military partners required a comprehensive approach allowing a wide spectrum of kinetic and non-kinetic responses, by both military and non-military actors. Essential to NATO's planning was the hypothesis that such a comprehensive response will have to be in partnership with other stakeholders, such as international and regional organizations, as well as representatives of business and commerce (Munoz Mosquera & Bachmann, 2016).

However, NATO's 2011 Concept of Hybrid Threats (CHT) and its visionary approach in regards to States, such as Russia, and their willingness to use the HW concept for aggressive purposes could not be developed further and as a result in June 2012 NATO decided to discontinue work on CHT on the organizational level in favor of member States. In autumn 2014, NATO reflected on the Russian aggression in Ukraine (including the occupation of Crimea) when declaring its resolution to get prepared for Russia's use of HW and Threats. During the Wales Summit Declaration of September 2014, NATO issued a statement that NATO is capable of addressing challenges posed by HW threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed and so the Alliance possesses the necessary tools and procedures required to deter and respond effectively to those threats (Munoz Mosquera & Bachmann, 2016).

This analysis results in the following remarks (Cullen, 2017, p. 4)

- HW is designed to exploit national vulnerabilities across the PMESII spectrum. Therefore as a minimum, national governments should conduct a self-assessment of critical functions and vulnerabilities across all sectors, and maintain it regularly.

- HW uses coordinated MPECI instruments of power that extend far beyond the military realm. National efforts should enhance traditional threat assessment activity to include non-conventional political, economic, civil, international (PECI) tools and capabilities tailored in a specific toolbox that diminish the vulnerabilities of a target.
- HW is synchronized and systematic and so national governments should establish and embed a process to lead and coordinate a national approach of self-assessment and threat analysis.
- Hybrid threats are an international issue. As a result, national governments should coordinate a coherent approach amongst themselves to understand, detect and respond to HW to their collective interests. Multinational frameworks, for a and working groups should be developed to facilitate cooperation and collaboration across borders.

5.4 EU-NATO Cooperation

EU-NATO cooperation has historically been marked by difficulties to agree at the political level, mainly due to the following reasons:

- Turkey is an ally (with difficult behavior) but a non-EU member posing at the same time certain requirements.
- Until 2008 France was not a member of the Integrated Military Command in NATO.
- The accession of Cyprus into the EU in 2004 was pursued even though the Greek-Turkish divergence on the status of the island remains unsolved and Turkey occupies illegally approximately the one third of the Cyprus territory since 1974 (Wieslander, 2016, p. 2).

For many years, the focus of institutional cooperation has been on crisis management and the so-called Berlin-Plus arrangements from March 2003 allows EU the usage of NATO planning and capabilities in crisis management operations. Though Berlin-

Plus yielded an immediate success for operations in Macedonia (2003) and Bosnia and Herzegovina (2004), since then collaboration in crisis management has overall been limited. Currently, NATO-EU partnership covers some concrete cooperation in the western Balkans, in Afghanistan, off the coast of Somalia and Libya and the East Aegean (migrant-refugee crisis). In the aftermath of the illegal Russian annexation of Crimea and war in eastern Ukraine, a new sense of urgency emerged regarding the need to develop cooperation between the EU and NATO in order to successfully counter hybrid threats (Wieslander, 2016, p. 2).

USA plays a significant role behind this reset. The underlying motive has been the need to strengthen the European contribution to the transatlantic relationship and the urge for EU to secure herself by her own means. The complementarity that has been developed among the organizations in past years has been reassuring from an American perspective. The UK has played a central role in balancing European and transatlantic forces, but due to Brexit, uncertainty has reemerged (Wieslander, 2016, p. 2).

Since 2014, both staff to staff level contacts, and contacts at the political level, have been increased substantially. NATO Secretary General Jens Stoltenberg had met several times with the former HR Federica Mogherini as well as with the former President of the European Council, Donald Tusk, and they have attended each other' s ministerial meetings on a frequent basis. Initially, there was an ambition to work side by side to develop strategies on how to deal with hybrid threats, and to some extent this was possible at staff level. However, in the end, NATO moved faster than the EU and approved a strategy on the first of December 2015 and an implementation plan on the 11th of February 2016, while the EU framework on countering hybrid threats did not land at the table of the Defense Ministerial Meeting until the 19th of April 2016. In the summer of 2016 at the NATO summit in Warsaw, NATO and the EU, the latter represented by both the former President of the EU Commission Jean-Claude Junker and Donald Tusk, issued a joint declaration as a landmark for establishing even closer cooperation. In the declaration, the organizations committed to:

> *"Boost our ability to counter hybrid threats, including by bolstering resilience, working together on analysis, prevention, and early detection, through timely information sharing and, to the extent possible, intelligence sharing between staffs; and cooperating on strategic communication and response. The development of coordinated procedures*

> *through our respective playbooks will substantially contribute to implementing our efforts* (Wieslander, 2016, p. 2).*"*

In addition, parallel and coordinated exercises on HW were planned for 2017 and 2018, and resilience of partners in the east and south are to be addressed including strengthening of maritime capacity (Wieslander, 2016, p. 2).

A wide range of areas have officially been identified for enhanced coordination and cooperation between NATO and the EU, including:

- Situational Awareness (SA).
- Information sharing.
- STRATCOM.
- Cybersecurity/cyber defense.
- Crisis prevention and response.
- Civil-military planning (Wieslander, 2016, p. 5).

For the abovementioned topics a playbook for NATO-EU cooperation, dealing with a range of HW scenarios, has been developed for the areas of cyber defense, strategic communications, SA and crisis management. The aim is to speed up decision making and to answer in advance questions about who does what (Wieslander, 2016, p. 5)

While both Jens Stoltenberg and Federica Mogherini had acknowledged that there was greater potential for more cooperation in helping partners to become more capable of securing themselves in Europe, the Middle East and North Africa, this has not yet been addressed in a systematic manner. However, in order to truly build resilience, enhanced NATO-EU cooperation should not be limited to member states. NATO and EU could combine resources and complement each other to deal with fragile and failed states, which are a very serious hybrid threat for West Democracy. A major challenge ahead would then be to efficiently coordinate defense building capacity support with development aid and economic support. Both Finland and Sweden are active contributors to support development in these regions through a broad range of policy areas, from development to the military, especially because these two states will also become NATO members in the close future. Sweden, together with Poland, took the initiative to start the Eastern Partnership (EP) within the EU in 2009 (Wieslander, 2016, p. 5-6).

The EU remains a much bigger player in terms of resources (funding and personnel) for partner cooperation. Nevertheless, the assessment of the EU Neighbourhood policy conducted during 2015 set the ground for a reapprochement between the institutions in two major ways: First, the EU is shifting its regional approach towards a more individualized effort towards countries, which is more in line with how NATO works. Secondly, the EU for the first time included security as an area of cooperation, thereby coming closer to the NATO agenda. In the latter, there is also a challenge when it comes to duplication, but a rough division of labour should work, based on NATO dealing mainly with the military aspects and the EU with the civilian. Areas of NATO focus include military training, democratic control of the armed forces (in the spirit of what Clausewitz believed), civil-military planning, counter-terrorism, and countering IED. These programs are in place for Jordan and Iraq, and could possibly be introduced also in Tunisia, Libya, and Morocco. The EU highlights civilian security sector reform, civil protection and disaster management, tackling terrorism and preventing radicalization, disrupting organized crime, fighting cybercrime, and chemical, biological, radiological and nuclear risk mitigation. The greater problem has to do with lack of coordination, information sharing, and exchange of assessments that would enable efficient resource pooling and a comprehensive approach to tackle fragility and vulnerabilities in a partner country (Wieslander, 2016, p. 6).

5.5 Conclusion

The fact that both Sweden and Finland are EU members, and as such could help promote further EU-NATO cooperation, has been highlighted but not yet fully explored in the Enhanced Opportunities Partnership (EOP). Sweden and Finland provide strong voices in the EU as contributors to crisis management and have a long tradition of involvement in neighbourhood issues. Thus, they can with credibility and competence assume leading roles in pursuing questions and issues of common interest. The EOP could be used to address the need to strengthen resilience in NATO and EU member states, as well as to the east and in the south. While there are good reasons to continue to keep a strong focus on Baltic Sea region security in the format of NATO, Sweden and Finland, (especially nowadays with the Russian Ukraine war) there are also arguments for broadening the agenda on resilience and make full use of the EU membership of the two partners. Another important aspect of opening up the EOP agenda is to avoid a perception of competition between sub-regions, such as the Baltic Sea and the Black Sea regions. Strengthened stability to the east and in the south promotes security for all, also in the north. NATO, the EU and partners could undertake additional actions to strengthen resilience within and beyond their borders and together face the continuous threat of HW (Wieslander, 2016, p. 6).

CHAPTER 6

Concluding Remarks

The art of HW is not found in front line manoeuvres, but rather in the zones of security that are grey, as this is the new colour of war. In the past, irregular tactics and protracted forms of conflict had mostly been marked as tactics of the weak and non-state actors who do not have the means to do better. Today and in the future, opponents may exploit hybrid opportunities because of their effectiveness. Unlike conventional warfare, the CoG in HW is the **individual**. The adversary tries to influence key policy and decision makers by combining kinetic operations with subversive efforts. The aggressor often resorts to clandestine actions to avoid attribution or retribution, introducing thus a type of warfare particularly dangerous to multiethnic societies (Thiele, 2015b).

Up to nowadays there are some lessons learned and identified by hybrid threats (Hoffman, 2009a, 2009b ; Thiele, 2015b):

- Mixed ethnic societies are particularly susceptible to mass and social media manipulation.
- Prior to conflict, subtle economic influence and the practice of corruption serve to establish leverage and achieve compromises from key politicians and security organizations.
- Political agents, volunteers and mercenaries provide a variety of low visibility insertion, sabotage, training and advisory options.
- Terrorist type techniques include building seizures, infrastructure attacks, intimidation of police, cyber disruption, political assassination, kidnapping of children, hostage taking, torture and mutilation.
- LIC that escalate rapidly to high-intensity warfare unveil unpreparedness of police, border guards, security units and even SOF teams to deal with these challenges.

- A variety of subtle and direct nuclear threats, including nuclear alerts and fly-bys reopen the nuclear debate.

HW will be a defining feature of the future security environment. This should widen the perspective of decision-makers and their interest to cooperate with relevant partners. Success in countering HW requires that political, military and civil echelon leaders be equipped with decision making and cognitive skills that enable them to recognize and quickly adapt to the unknown. Organizational learning and adaptation is of importance, as is investment in training and education. To this end, nations and defense organizations need to make far better use of lessons identified and learnt in recent campaigns. But the training and education should be also prioritized by the society as a whole. Children at school should first learn the values of democracy, freedom of speech, respect and liberty. In addition to, they should learn to use properly the advantages of technology and be aware of its dangers, such as misinformation and disinformation, especially in areas of high importance, such as the ridiculous and lethal antivaccination campaign during the Covid-19 pandemic (Thiele, 2015b).

These lessons should be incorporated into a programme in which future capabilities will meet hybrid challenges via a series of linked exercises and security education initiatives. Exercise and training programmes need to be adapted to reflect recent developments in and reactions to hybrid warfare (Thiele, 2015b).

Early indicators[1] should be established to enable more agile responses to hybrid threats, especially in the early phase of the conflict cycle. To counter complex hybrid challenges, nations – individually and within an allied e.g. EU-NATO framework – should firstly:

- Determine how to best promote democracy, human rights, and the rule of law.
- Emphasize transparency and due process across all elements of society.
- Strengthen cooperative regional approaches that build support for like-minded partners.

The nature of HW is such that it is difficult to know whether we are still in times of peace or already at war period. Unpredictability has become a weapon. Up to now

[1] *Hybrid COE expert pool meeting on cyber, "The future of cyberspace and hybrid threats", Hybrid CoE Trend Report 6, April 2021 ,pgs. 16, 17.*

approaches countering HW have been centered on rapid military responses. This approach has weaknesses, particularly in alliances, when member states need to agree and the debate of which constitutes a significant barrier to rapid collective action .

On the other side, hard power may prove insufficient to counter hybrid threats. The military instrument per se plays an important but limited role. The challenge is to orchestrate the balanced employment of all of the instruments of power: Diplomacy, Information, Military and Economic (DIME). This highlights the need for a broadbased approach, using (Thiele, 2015b):

- Rapid deployment and power projection.
- SOF and cyber operations.
- Intelligence operations and police investigations.
- Financial and economic measures.
- Information and social media campaigns.

Such a broad spectrum of instruments cannot come from a single source, from a single nation or a single organization. Consequently, within any HW strategy specific consideration must be given to the role of partner nations and organizations, regarding how best to enhance not only one's own resiliency but also that of Allies and Partners. Particular focus should be put on the protection of critical national information and infrastructures as well as on consequence management. A useful first-step could be an analysis of key vulnerabilities to better understand how individual nations could be undermined by HW. Such an analysis would include a better understanding of:

- How minorities are susceptible to manipulation.
- How vulnerable media are to external saturation.
- How the lack of a binding national narrative could be exploited.
- How electorates could be alienated from leadership during a HW-inspired crisis, particularly through elite corruption (Thiele, 2015b).

HW presents also considerable institutional challenges to both domestic defense capabilities and wider security alliances. NATO for instance will need to strengthen cooperation with international organizations and partners such as has already done with the EU. The NATO Summit in Wales has already acknowledged the EU as a strategic partner.

The common threat of HW within the Euro-Atlantic area presents a solid opportunity to develop this partnership. NATO and the EU could create an effective institutional tandem that has a wide range of diplomatic, information, military and economical instruments at its disposal. (Thiele, 2015b).

As Frank G. Hoffman states:

"The rise of HW does not represent the defeat or the replacement of "the old-style warfare" or conventional warfare by the new. But it does present a complicating factor for defense planning in the 21st Century. Future adversaries will not offer up "tactics of the weak" and operate in distant mountain retreats. They will exploit the tactics of the smart and agile, presenting greater reach and lethality. They may attempt to operate within heavily populated cities, and use the networks of an urban metropolis to maneuver within as well as to sustain themselves (Hoffman, 2009, p. 38).*"*

Of course there is an upmost need in changes to be done in several domains of the civil-military response to HW mainly found at (Thiele, 2015b):

- Force planning.
- Intelligence.
- Interagency Approach.
- Organizational Culture/Ethos.
- Doctrine.
- Training and Education.
- Operational Planning/Campaign Design.
- Dueling Narratives.

Finally, the rise of HW does not represent the end of traditional or conventional warfare, but a complicating factor for defense planning in the 21st century. Any force prepared to address hybrid threats would have to be built upon a solid professional military foundation with a premium on the cognitive skills needed to recognize or quickly adapt to the unknown. Decision makers and militaries may have to redouble their efforts to revise operational art as they have mastered operational design for conventional warfare and recently reinvigorated their understanding of counterinsurgency campaigns, by firstly answering the following questions (Hoffman, 2009, p. 38):

- What is the CoG in such conflicts, and does it invalidate emphasis on whole-of-government approaches and lines of operations?
- What institutional mechanisms do we need to be more adaptive, and what impediments does our centralized—if not sclerotic—Defense Department generate that must be jettisoned?

Success in HW also requires small unit leaders with quick decision making skills and tactical cunning to respond to the unknown and the equipment sets to react or adapt faster than tomorrow’s foe. Organizational learning and adaptation would be at a premium, as would extensive investment in diverse educational experiences. The greatest implications will involve force protection. Hybrid enemies will focus on winning the mobility-counter mobility challenge to limit their opponent’s freedom of action and separate officers from close proximity to the civilian population. The ability of hybrid challenges to exploit the range and precision of various types of missiles, mortar rounds and mines will increase over time (Hoffman, 2009a, p. 38).

Learning cycle has already been seen in Iraq and Afghanistan, as USA insurgents appeared to acquire and effectively employ tactical techniques or adapt novel detonation devices found on the Internet or observed from a different source. These opponents will remain elusive, operate in an extremely distributed manner and reflect a high degree of opportunistic learning. The U.S. military and indeed the armed forces of the West must adapt as well (Hoffman, 2009a, p. 38).

Yet the focus remains on an outmoded and dated bifurcation of war forms and this orientation overlooks the most likely and potentially the most dangerous of combinations. Respected strategists have concluded that HW will be a defining feature of the future security environment. If true, a wider and more difficult range of threats will be uncovered. As today’s Spartans, there is a high need to take the enemy’s plans into consideration and adapt into a more multidimensional or joint force as Sparta ultimately did. Today’s strategists must remember the frustrated Spartans outside Athens’ long wall and remember the Pyrios’ victories of the British, Russians and Israelis in their long wars against hybrid threats and so prepare accordingly (Hoffman, 2009a, p. 39).

References

In Greek Language

Koliopoulos, K. (2008). *Strategic Thinking: From the ancient years up to the present.* Athens: Poiotita.

Konstantopoulos, I. (2020). Hybrid Warfare and Information. *Hellenic Airforce Review, 118* .

Konstantopoulos, I. (2010). *Economy and Espionage: Theory and Practices.* Athens: Poiotita.

Platias, A. (1995). *The new World System: Realistic Approach of International Relations.* Athens: Papazisis.

Platias, A. (2012). Geopolitics, Geoeconomy and International Competition. In *Honorary Volume of Professor Emeritus Karvounis, S.* (σσ. 591-622). Piraeus: Research Center of the University of Piraeus.

Platias, A. (2020). *International Relations and Strategy on Thucydides. 8th Edition.* Athens: Estia.

Platias, A., & Koliopoulos, K. (2015). *The art of War of Sun Tzu.* Athens: Diavlos .

Thucydides (1940). *Thucydides History. Edition: Political Subjects. (Translation: Venizelos, El.)* .

In English Language

Abdyraeva, C. (2020). The Use of Cyberspace in the Context of Hybrid Warfare: Means, Challenges and Trends. *(Working Paper / Österreichisches Institut für Internationale Politik, 107). Wien: Österreichisches Institut für Internationale Politik (oiip)*. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-69232-1.

Andersson, J., & Tardy,T. (2015). Hybrid: what's in a name? *European Union: Institute for Security Studies, Brief Issue 32/2015* , p. 2.

Brattberg, E., & Maurer, T. (2018). Five European Experiences With Russian Election Interference. *Carnegie Endowment for International Peace*. https://www.jstor.org/stable/pdf/resrep21009.6.pdf.

Burbridge, D. A. (2013). *Employing U.S. Information Operations Against Hybrid Warfare Threats.* Pennsylvania: United States Army War College.

Clausewitz, C. (2007). *On War.* Oxford University Press.

Cullen, P. J. (2017). *Understanding Hybrid Warfare. MCDC Countering Hybrid Warfare Project.* Retrieved from από MCDC: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

ECCC. (2022). *European Cybersecurity Competence Centre and Network*. Retrieved from European Cybersecurity Competence Centre: https://cybersecurity-centre.europa.eu/about-us_en

European Commission . (2018). *European Commission contribution to the European Council. Action Plan against Disinformation.* Retrieved from https://ec.europa.eu/info/sites/default/files/eu-communication-disinformation-euco-05122018_en.pdf

European Commission. (2022a). *Internal Market, Industry, Entrepreneurship and SMEs*. Retrieved from European Commission website: https://ec.europa.eu/info/departments/internal-market-industry-entrepreneurship-and-smes_en#responsibilities

European Commission. (2022b). *Migration and Home Affairs*. Retrieved from European Commission Website: https://ec.europa.eu/info/departments/migration-and-home-affairs_en

European Commission. (2022c). *Joint Research Centre*. Retrieved from European Commission website.

European Commission. (2020b). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

European Commission. (2020a). *The EU's cybersecurity stragedy for the digital decade*. Retrieved from https://privacy-web.nl/wp-content/uploads/po_assets/559579.pdf

European Union. (2022b). *European Defence Agency (EDA)*. Retrieved from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/eda_en

European Union. (2022a). *European External Action Service (EEAS)*. Retrieved from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/eeas_en

European Union. (2022c). *European Union Agency for Law Enforcement Cooperation (Europol).* Retrieved from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/europol_en

Europol. (2022). *EU Internet Referral Unit - EU IRU*. Retrieved from https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru

Fitzgerald, M., & Lebow, R. (2006). Iraq: The Mother of all intelligence failures. *Intelligence and National Security, 21(5)* , pp. 884 – 909. DOI: 10.1080/02684520600957811.

Fleming, B. (2011). *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art.* Fort Leavenworth, Kansas: School of Advanced Military Studies United States Army Command and General Staff College.

Freedman, L. (2014). Ukraine and the Art of Crisis Management. *Survival, 56(3)* , pp. 7-42, DOI: 10.1080/00396338.2014.920143.

Giegerich, B. (2016). Hybrid Warfare and the Changing Character of Conflict. *Connections: The Quarterly Journal. 15(2)* , pp. 65-72. http://dx.doi.org/10.11610/Connections.15.2.05.

Gilbert, F. (1986). Machiavelli: The Renaissance of the Art of War. In P. Paret, G. A. Craig, & F. Gilbert, *Makers of Modern Strategy from Machiavelli to the Nuclear Age.* Princeton University Press.

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington, Virginia, USA: Potomac Institute for Policy Studies.

Hoffman, F. G. (2009b). Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. *Strategic Forum 240* , pp. 1-9. https://www.files.ethz.ch/isn/98862/SF240.pdf.

Hoffman, F. G. (2009a). Hybrid Warfare and Challenges. *Joint Force Quarterly 52* , σσ. 34-48. https://apps.dtic.mil/sti/pdfs/ADA516871.pdf.

Hoffman, F. G. (2010). Hybrid Threats': Neither Omnipotent Nor Unbeatable. *Orbis 54(3), Oxford-England: Elsevier Science on behalf of Foreign Policy Research Institute* , pp. 443-444.

Hunter, E., & Pernik, P. (2015). The Challenges of Hybrid Warfare (Analysis). *Estonia-Talin:International Centre for Defence and Security* .

Huovinen, P. (2011). *Hybrid Warfare. Just a Twist of Compound Warfare? Views on warfare from the United States Armed Forces perspective.* Retrieved from Department of Military History: https://www.doria.fi/bitstream/handle/10024/74215/E4081_HuovinenKPO_EUK63.pdf?sequence=1&isAllowed=y

Hybrid CoE. (2021). *The future of cyberspace and hybrid threats. Hybrid CoE Trend Report 6.* https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210407_Hybrid_CoE_Trend_Report_6_The_future_of_cyberspace_and_hybrid_threats_WEB.pdf.

Johnson, D. (2010). *Military Capabilities for Hybrid War:Insights from the Israel Defense Forces in Lebanon and Gaza.* Retrieved from RAND Corporation: https://www.rand.org/content/dam/rand/pubs/occasional_papers/2010/RAND_OP285.pdf

Kert-Saint Aubyn, M. (2022). *EU Policy on Fighting Hybrid Threats*. Retrieved from

CCDCOE: https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats/

Kober, A. (2008). The Israel defense forces in the Second Lebanon War: Why the poor performance? *The Journal of Strategic Studies 31(1)* , pp. 8-9.

Kofman, M. & Rojansky, M. (2015). A Closer look at Russia's "Hybrid War. *Kennan Cable 7* , pp. 1-8.

Kramer, F. D., & Speranza, L. M. (2017). Meeting the Russian Hybrid Challenge: A Comprehensive Strategic Framework. *Atlantic Council Reports* , pp. 1-29.

Liaropoulos, A. (2019). Russian Information Operations: A Pillar of State Power. In C. Filis, *A Closer Look at Russia and its influence on the World* (pp. 191-202). Nova Science Publishers.

Mansoor, P. (2012). Introduction: Hybrid Warfare in History. In W. Murray, & P. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (pp. 3-4). Cambridge University Press.

Mattis, J., & Hoffman, F. (2005). Future Warfare: The Rise of Hybrid Wars. *U.S. Naval Institute Proceedings Magazine, Vol. 132/11/1,233* , pp. 1-2.

McCulloh, T., & Johnson, R. (2013). *Hybrid Warfare*. Retrieved from https://www.hsdl.org/?view&did=744761

Minzarari, D. (2022). *The next war: How Russian hybrid aggression could threaten Moldova.* Ανάκτηση November 22, 2022, από European Council on Foreign Relations (ECFR): https://ecfr.eu/publication/the-next-war-how-russian-hybrid-aggression-could-threaten-moldova/

Monaghan, S. (2019). Countering Hybrid Warfare: So What for the Future Joint Force? *Prism 8(2)* , pp. 83-98.

Mueller, R. S. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* . Washington, D.C. : U.S. Department of Justice .

Mumford, A. (2016). *The Role of Counter Terrorism in Hybrid Warfare (Report).* UK: NATO's COE DAT: University of Nottingham.

Munoz Mosquera, A. B., & Bachmann, S. D. (2016). Lawfare in Hybrid Wars: The 21st Century Warfare. *Journal of International Humanitarian Legal Studies, 7(1)* , pp. 63-87. doi: https://doi.org/10.1163/18781527-00701008.

National Security Authority. (2020). *EU has presented a new cybersecurity strategy*. Retrieved from https://www.nbu.gov.sk/news/eu-has-presented-a-new-cybersecurity-strategy/index.html

Odote, P.O. (2016). *Role of early warning systems in conflict prevention in Africa: Case study of the Ilemi Triangle. PhD Thesis.* Nairobi: University of Nairobi.

Otaiku, A. (2018). A Framework for Hybrid Warfare: Threats, Challenges and Solutions. *Journal of Defense Management 8(3),* p. 2. doi: 10.4178/2167-0374.1000178.

Pacepa, I. M., & Rychlak, R. (2013). *Disinformation* . US: WND Books.

Pana, M. (2016). Hybrid Confrontation: Hezbollah - a case study. *PROCEEDINGS. The 12th International Scientific Conference STRATEGIES XXI. 'Strategic Changes in Security and International Relations', National Defense University, CAROL I, Bucharest, Romania* , pp. 66-71.

Platias, A., & Koliopoulos, K. (2010). *Thucydides on Strategy: Grand strategies in the Peloponnesian War and their relevance today*. Columbia University Press/C. Hurst & Co Publishers Ltd.

Platias, A., & Trigkas, V. (2021). Unravelling the Thucydides' Trap: Inadvertent Escalation or War of Choice? *The Chinese Journal of International Politics, Vol. 00, No. 0* , pp. 1-37. doi: 10.1093/cjip/poaa023.

Reichborn-Kjennerud, E., & Cullen, P. (2016). What is Hybrid Warfare? *Norwegian Institute of International Affairs, Policy Brief [1/2016]* .

Richterová, J. (2015). NATO Hybrid Threats. *Background Report, PRAŽSKÝ STUDENTSKÝ SUMMIT/XXI/NATO/III* .

Rietjens, S. (2020). A warning system for hybrid threats – is it possible? *Hybrid CoE Strategic Analysis 22* , pp. 2-8.

Rupert, J. (2015). *Russian Troops Lead Moscow's Biggest Direct Offensive in Ukraine*

Since August. Retrieved from Atlantic Counsil: https://www.atlanticcouncil.org/blogs/ukrainealert/russian-special-forces-and-regular-troops-lead-moscow-s-biggest-direct-offensive-in-ukraine-since-august/

Snegovaya, M. (2015). Russia Report 1. Putin's Information Warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare. *United States of America:Institute for the Study of War* . https://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

Thiele, R. (2015a). Crisis in Ukraine – The Emergence of Hybrid Warfare. *ISPSW Strategy Series: Focus on Defense and International Security 347* , pp. 1-13.

Thiele, R. D. (2015b). The New Colour of War. Hybrid Warfare and Partnerships. *ISPSW Strategy Series: Focus on Defense and International Security 383* , pp. 1-12. https://www.files.ethz.ch/isn/194330/383_Thiele.pdf.

Waltz, K. (2011). *Theory of International Politics.* Athens: Poiotita.

Wieslander, A. (2016). *Forward Resilience: Protecting Society in an Interconnected World. How NATO and the EU can Cooperate to Increase Partner Resilience.* Retrieved from Center for Transatlantic Relations: https://archive.transatlanticrelations.org/wp-content/uploads/2016/12/resilience-forward-book-wieslander-final.pdf

Wither, J. K. (2016). Making Sense of Hybrid Warfare . *Connections, 15(2)* , pp. 73–87. http://www.jstor.org/stable/26326441.

Wolf-Diether, R. (2019). *Resilience: the first line of defence.* Retrieved from NATO Review: https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html