The EU Joint Framework on Countering Hybrid Threats and its effect on the Dutch approach on Hybrid Threats

Leiden University- Campus The Hague

Faculty of Governance and Global Affairs

Master Crisis and Security Management

Bas Lippe

S1794485

Table of Contents

1 Introduction 4

1.1 A positive future? 4

1.2 The new threat 5

1.3 Is the new threat real? 6

1.4 Central Research Question 6

1.5 Academic and Societal Relevance 7

1.6 Link to Crisis and Security Management 9

1.7 Reading Guide 9

2 Hybrid Warfare and the evolution 11

2.1 Introduction of the concept 11

2.2 The founders of the concept 12

2.3 An intermezzo 14

2.4 Hybrid only for the underdog? 15

2.5 Adding more aspects to the concept 15

2.6 Hybrid War and Russia 16

2.7 Even more holistic 19

2.8 EU and Hybrid 22

2.9 Summary of the evolution of Hybrid Warfare 23

3 Hybrid Warfare, a truly new and scary phenomenon? 24

3.1 Hybrid Warfare and realism 24

3.2 Hybrid Warfare as vehicle to create own possibilities 26

3.3 Hybrid Warfare and cyber 28

3.4 Stay calm, despite the threat 29

4 Methodology 31

4.1 Introduction 31

4.2 Definition 31

4.3 Research Design 31

4.4 Operationalisation 32

4.5 Data collection 33

4.6 Analyses 35

4.7 Boundaries 36

4.8 Validity 37

5 The European Union and Hybrid 38

5.1 The EU takes an interest in Hybrid Threats 38

5.2 Joint Framework on countering Hybrid Threats: an overview 40

5.3 Implementing the Joint Framework, what has been achieved in year 1? 42

5.4 Implementing the Joint Framework, what has been achieved in year 2? 44

5.5 From Union towards member state 45

6 Findings and Analysis. 47

6.1 Introduction 47

6.2 Indicator: The concept of Hybrid Threats is incorporated in policy documents. 47

6.3 Indicator: Budgets are assigned to counter Hybrid Threats 52

6.4 Indicator: National or international organisational elements dealing with Hybrid Threats are (being) established. 54

6.5 Indicator: National or international coordination structures on Hybrid Threats are (being) established. 56

6.6 Further remarks by the respondents 58

7 Conclusion and Discussion 59

7.1 Conclusion 59

7.1.1 The extent to which the EU initiatives on Hybrid have influenced the Dutch approach is very limited. 59

7.1.2 How to explain the limited influence. 59

7.2 Discussion 60

8 Abbreviations 63

9 References 64

9.1 Authors 64

9.2 EU publications 67

9.3 Dutch documents 67

1 INTRODUCTION

1.1 A POSITIVE FUTURE?

Since the end of the second World War the two superpowers, the communistic Soviet Union (SU) and the liberal United States (US), helped to maintain the post-war peace. Roughly, there was military equality, both in conventional troops as in nuclear weapons, thus creating the notion that is was impossible to win a conventional war against the other. And even if a conventional war could be won, the other did possess a huge nuclear arsenal which would be used to retaliate[1]. This form of peace was known as the Cold War. But this peace was based on mutual threat and divided the world in two separate blocks. And although the confrontation of different social values, economic and personal liberties and political systems never led to open conflicts, the tension between the two sides was very clear.

The fall of the Berlin Wall in November 1989 can be seen as the beginning of the end of the Cold War. In the West it was celebrated as the clear victory of Western liberal values[2]. Now the communists had realised that their system was wrong and that liberal democracy was the only way forward, the threat of war would disappear. After all, the liberal international economic order requires a peaceful and stable world in order to flourish, and liberal democracies do not fight each other[3]. Fukuyama even declared it "the end of history", assuming that now one single social system would develop, that would mark the end-point of humanity's sociocultural evolution and would be the final form of human societal organisation. Unfortunately this assumption was as optimistic and as unrealistic as Chamberlains "Peace for our time" declaration in 1938. After signing a pact with Hitler, allowing him to annex those parts of Czechoslovakia that where populated by ethnic Germans, Chamberlain was convinced that Europa would know peace for decades to come. Hitler however, broke the treaty within in a year, and invaded Poland on September 1st 1939. Also the 90's new optimistic view did not last long.

[1] John J. Mearsheimer, Back to the Future: Instability in Europe after the Cold War, International Security, Vol. 15, No. 1 (Summer, 1990), p. 5-7.

[2] Salome Samadashvili, Muzzling the Bear, Strategic Defence for Russia's Undeclared Information War on Europe, Wilfried Martens Centre for European studies, 2014, p.15.

[3] John J. Mearsheimer, Back to the Future: Instability in Europe after the Cold War, International Security, Vol. 15, No. 1 (Summer, 1990), p. 8.

1.2 THE NEW THREAT

It is hard to tell when the new optimistic worldview ended, but events like the occupation of Kuwait by Iraq (1990 – 1991), the violent brake up of Yugoslavia (1991 – 2001) and the Russian invasions of Chechnya (1994 – 2000), soon made it clear that global peace was still far away. The 9/11 attacks on the US brought the devastating effects of well-coordinated terrorism to Western soil. During the following invasion of Afghanistan and Iraq, two countries that are part of the "axis of evil[4]", the US and her allies initially fought against regular troops. But once these were defeated, the fighting did not stop. The coalition found itself confronted with highly motivated and fanatic clans, warlords, organised crime gangs and terrorist groups like Taliban and al Qaida. Such groups were not fighting a classical inter-state war, of course not after all they are non-state actors, but were using intra-state violence in order to achieve their goals. They showed no respect for the *jus in bello*[5] and projected their violence not only against the alliances forces, but also against the population[6]. This turned out to be very effective to undermine the four pillars of stable peace: security, social and economic well-being, justice and reconciliation, and governance and participation[7].

The world realised that a new form of warfare was emerging. A form in which both state and non-states actors use multidimensional campaigns, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary. These campaigns are designed to be difficult to detect or attribute[8]. By using non-military means like political and economic pressure, by deploying terrorists or warlords rather than regular troops when the use of force is necessary, by creating confusion and setting up the population against their government by using the global reach of cyberspace, it is possible to undermine societies without crossing the threshold of an armed conflict. This new form of warfare was named Hybrid Warfare.

As will be shown in chapter 2, the concept of Hybrid Warfare has multiple faces and is still developing. Once the dangers of Hybrid Warfare were recognised, scholars, thinktanks and security organisations started to develop concepts on protective measures against it. The EU is

[4] States and their terrorist allies that pose a threat to world peace. George W. Bush, State of the Union 2002, https://georgewbush-whitehouse.archives.gov/news/releases/2002/01/20020129-11.html

[5] See chapter 3.2 for a short description.

[6] Laura-Maria Herta, Hybrid Warfare – a form of asymmetric conflict, International Conference Knowledge-Based Organization Vol. XXIII No 1 2017, p. 136.

[7] Hans Binnendijk, and Stuart E. Johnson, Transforming for Stabilization and Reconstruction Operations, Center for Technology and National Security Policy, National Defense University, Washington, DC, 2004, p. 90.

[8] JOIN(2018) 16 final, Increasing resilience and bolstering capabilities to address hybrid threats, Brussels, 13.6.2018, p. 1.

one of the organisations that put Hybrid Warfare on the agenda. Although the term Hybrid Warfare was already used in the beginning of this century, it took until 2016 before the EU issued a document that should help member states to protect themselves and the Union against Hybrid Threats. Now, 2 years after the release of the Joint Framework on countering Hybrid Threats, the EU has issued two annual reports on the progress. In both reports “significant” progress is claimed.

1.3 IS THE NEW THREAT REAL?

But not all research done on Hybrid Threats concludes that these threats are actually new and have the impact that is suggested. A group of scholars does not think that Hybrid Threats force the Western world to change their view on security and to adjust security policies. In chapter 3 will be explained that many of the threats we are confronted with today are threats we have been struggling with for decades. It is acknowledged that more actors have entered the “conflict-arena”, that states are no longer the sole competitors, that technological developments have increased the capabilities for even the smallest contester, that the lines between war and peace have been blurred, that recognisable concepts like a FLOT[9] are hardly ever found and battles are often fought in populated areas. The security environment has become more complex, that is true, but in the end it is still about achieving goals, often at the expense of others. The criticasters suggest that there other reasons why the concept of Hybrid Threat is gaining popularity. Uzieblo and Tennenbaum suggest that it is used as leverage in the discussion over limited budgets[10]. Even within the Dutch military some whisper that the NATO reporting on Russia is exaggerated in order to re-create an enemy, capable of threatening NATO’s borders. This image of a new enemy is used to get higher budgets assigned to the military.

1.4 CENTRAL RESEARCH QUESTION

This thesis is not about the content or the boundaries of the concept of Hybrid Threats. It aims to determine to what extend the new security challenge “Hybrid Threat” has led to structural adjustment of security policies. Or in other words: to what extend is the concept of Hybrid Threats been accepted. This will be done by examining to what extend one member state,

[9] Forward Line Own Troops. A very clear military concept, in simple words: a line on the map; everything on the other side is enemy and can be engaged.

[10] See chapter 3.

namely the Netherlands, has actually implemented the EU policy, or made adaptations to their security strategy, as advocated at EU level. This leads to the following research question:

> ***To what extent have the EU-initiatives on Hybrid Threats influenced the Dutch approaches and how to explain for the (relatively) presence or absence of such an effect?***

The EU initiatives has been chosen as a starting point for several reasons. First of all, Hybrid Threats ignore territorial boundaries, Such threats can be countered more effectively with a coordinated response at EU level[11]. Next, the preferred partner in defence issues has been NATO. The last years, however, the relations with the US are changing; the US is charging import taxes, not only to China and India, but also to NATO members and the EU; NATO members are being criticised for not spending enough on defence and the US has indicated that it will no longer automatically take the lead when in the international community considers it essential to intervene in a conflict[12]. These changes have opened a window of opportunity for the EU to pick up a more prominent role in security, and they did. One of the EU security initiatives is on Hybrid Threats, for which a concrete policy has been developed. Not only is the EU claiming a bigger role in security, this increasing importance of the EU is actually acknowledged by the member states.

It is my assumption that if the Netherlands is working on an own national policy on Hybrid Threats, and that this policy reflects the actionable items as proposed by the EU, the Netherlands acknowledges Hybrid Threats to be real threats *and* considers the EU initiatives to be meaningful.

1.5 Academic and Societal Relevance

Hybrid Warfare is considered to be something new which makes it worth studying[13]. And it has been studied, as will be shown in chapter 2 and 3. These studies were not only about what Hybrid Warfare is, but also ways to protect against Hybrid Threats were explored. Most of the suggested ways of defending against Hybrid Threats are food-for-thought concepts. They are written down in rather vague statements, lack tactics and procedures that will make them effective, and do not offer any starting point for developing criteria to measure the

[11] See also chapter 5.2.

[12] For example, in 2011 when UN Security Council Resolution 1973 (2011) called for intervention in Libya, NATO responded, but Operation Uniffied Protector was led by France and the United Kingdom.

[13] Guillaume Lasconjarias and Jeffrey A. Larsen, Introduction: A New Way of Warfare, in Guillaume Lasconjarias and Jeffrey A. Larsen, NATO's Response to Hybrid Threats, NATO Defense College, Forum Paper 24, 2015, p.1.

effectiveness. For example; in the NATO Capstone Concept, under the header "Building Partnerships and Knowledge" it is stated that "the Alliance would seek to identify and engage prominent actors (including International Organizations, Private Organizations, key empowered individuals and Non-Governmental Organizations) whilst developing its own regional (and cultural) understanding[14]." A pretty holistic approach, but what end-state will be satisfying, and how can that be measured?

As will be shown in chapter 3, certain scholars criticise the concept of Hybrid Threats and its usability. From an academic point of view it is interesting to make the complex concept tangible and to see whether initiatives taken by the EU can indeed guide member states in their own process of dealing with Hybrid Threats.

The EU Joint Framework does not only offer "actionable items", but it also provides annual updates of the progress that the EU feels that it is making. These progress reports make it possible to compare the EU view on the progress with the progress made by member states. The academical relevance of this study is that this will be the first empirical check whether the EU policy on countering Hybrid Threats is indeed implemented by a member state as intended. This study will only cover one member state, and might be a trigger for other scholars to duplicate this to see whether the findings of this study are shared within the Union.

The societal relevance is twofold. The EU is a large bureaucratic organisation that has great influence on everyday life in member states. Often it is heard that the EU is much too expensive and does not deliver useful policies. The first thing that this study will examine is whether the efforts made, and the money spend, by the EU on this part of the security agenda can be considered as money well spent, and prove the added value the EU has in countering Hybrid Threats. The second part of societal relevance is about threat reduction. Hybrid Threats can be released upon societies in multiple forms and from multiple angles. This makes them hard to recognise, thus creating a vague, uncomfortable feeling of insecurity amongst both policy-makers and citizens. Proving that proposed policies are being implemented and effective will reduce this feeling. For citizens this means that they can sleep quietly. For policy-makers it should be a reassurance that they are doing the right things in

[14] BI-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats, 1500/CPPCAM/FCR/10-270038 5000 FXX 0100/TT-6051/Ser: NU0040, August 2010. www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

order to provide security to the population and encourage them to continue, or even step-up, their efforts.

1.6 Link to Crisis and Security Management

Security is nowadays being challenged in many different ways. Climate chance might be threating the survival of mankind in total, huge migration streams from Africa and the Middle East towards Europe do threaten our wealth and create cultural tension. Freshwater and essential raw materials are getting more and more scarce which increases the chance that open (armed) conflicts will arise in order to acquire those resources. Organised crime does not stop at territorial boundaries but has formed global networks that penetrate and disrupt societies. Non-state actors like Islamic State of Iraq and Syria (ISIS) do not limit their violent actions to their self-proclaimed kalifate, but are actively trying to radicalise and recruit young people throughout the world in order to spread their terrorist actions on a global scale. The giant progression made in communication technology, and the enormous worldwide availability of internet, the dependency of developed countries on cyber, and easy-to-use software (in particular social media, but also software that can disrupt cyberspace) made it simple to spread disinformation that creates confusion and undermines peoples trust in their governments. Some state actors demonstrate a new geopolitical ambition, like the wish of Russia to become a world power again and the efforts of China to gain control over the South Chinese See. These ambitions put pressure on existing status quo and stability. These threats by themselves are already reason enough to get worried, but it gets real complicated when actors, both state and non-state, deliberately start deploying multiple threats in order to achieve strategic goals, which is called Hybrid Warfare.

The aim of the Master Crisis and Security Management is to provide insight in contemporary threats to security and ways to manage them and to mitigate the effects. This thesis will cover the concept Hybrid Warfare, a topic that has received high priority on the security agenda of many states and organisations. It explores to what extend concrete actions are taken by the EU and a member state (i.e. The Netherlands) to counter these threats and to mitigate the effects.

1.7 Reading Guide

After this introductory chapter, in chapter 2 the body of knowledge on the concept of Hybrid Threat, and it’s developments, will be explored. In this chapter only authors that see Hybrid as new and as a real threat are used to explain the concept. In chapter 3 the concept will be addressed again, but this time from a more critical perspective. This time authors that doubt whether it is as new and as threatening as claimed in chapter 2, are used. Chapter 4 will explain the used methodology, the data collection and the analysis. In chapter 5, an overview of the EU activities on Hybrid Threats will be given, as well as a summary of the progress made. This will clarify the advocated EU policy and initiatives, and will act as the starting point to compare the Dutch initiatives. In chapter 6 the findings of this research will be presented. In the last chapter the R.Q. will be answered. It will also contain a discussion on the subject.

2 HYBRID WARFARE AND THE EVOLUTION

"The international consensus on 'hybrid warfare' is clear: no-one understands it, but everyone, including NATO and the EU, agrees it is a problem.[15]"

2.1 INTRODUCTION OF THE CONCEPT

Hybrid Warfare has become an hot item in the international security environment. Many scholars have published articles on this subject, it has found its way to the security agendas of both NATO and EU, think tanks and Centres of Excellence have embraced the topic. But despite all the attention it receives, still no-one understands it and, so far, no agreed definition has emerged[16]. Since the introduction of the term Hybrid Warfare in 2002, all the research and publications did not lead to a convergence of opinions and the fine-tuning of the concept. The more the term Hybrid Warfare was adopted, the more it was exposed to stakeholders with their own specific security policies. A clearly defined concept is not in the interest of these stakeholders since "[e]ach member state, sub-agency or centre of excellence understood [hybrid warfare] its own way, so that they could use it to push their own agenda"[17]. With these different stakeholders came a variety of definitions and descriptions of the concept. Apart from all the differences, most of the definitions "agree that it connotes a combination of different means and methods of strategy and warfighting that undermines the utility of the traditional Western analytical categories of conventional and irregular war. There is also general agreement that Hybrid Warfare extends itself to include other forms of competitive human interaction, such as the economy, information, diplomacy, criminality and terrorism"[18].

This chapter will describe the evolution of the concept since its first appearance in 2002. It has no intention to come up with all-inclusive definition that can be universally applied, it is only used to illustrate the complexity of the concept.

[15] Patrick J. Cullen & Erik Reichborn-Kjennerud, "Countering Hybrid Warfare (CHW) Analytical Framework", Multinational Capability Development Campaign (MCDC), 1 October 2016, p. 3.

[16] Jan Jakub Uziebło, "United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats", EU Diplomacy Papers 5/2017, p. 4.; Patrick J. Cullen & Erik Reichborn-Kjennerud, "Countering Hybrid Warfare (CHW) Baseline Assessment", Multinational Capability Development Campaign (MCDC), 1 October 2016, p. 4.; Katie Abbott, "Understanding and Countering Hybrid Warfare: Next Steps for the North Atlantic Treaty Organization", University of Ottawa, March 23, 2016, p. 2.

[17] K. Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power", Chatham House Research Paper, London, RUSI, 2016, p. 7.

[18] Patrick J. Cullen & Erik Reichborn-Kjennerud, "Countering Hybrid Warfare (CHW) Baseline Assessment", Multinational Capability Development Campaign (MCDC), 1 October 2016, p. 4.

2.2 THE FOUNDERS OF THE CONCEPT

As on the exact meaning of the term Hybrid Warfare, there is discussion about the moment it first appeared. Many scholars claim that Frank Hoffman introduced the term in 2006. In my opinion William Nemeth was the first to use the term in 2002 in his study *Future War and Chechnya: A Case for Hybrid War*[19]. In this study Nemeth compares loosely organised, clan and tribe based pre-state societies, to tightly organised, centrally controlled modern societies, and the way they fight wars[20]. Hybrid societies, he claims, are a mixture of the pre-state and the modern society. Being in the middle, a hybrid society has access to both traditional ways of warfighting as well as to modern ways; hybrid societies have hybrid forces. Although he does not clearly make the connection himself, it is logical to assume that the way these hybrid forces fight, can be called Hybrid Warfare. Nemeth sees Hybrid Warfare as an advanced way of guerrilla warfare that uses modern technology and mass media to exploit certain weaknesses of modern forces[21]. In Chechnya basically every available form of force was used to defend the country against the invading forces of Russia. The central government had limited military forces at its disposal, these were used in combat. But the main achievement was to coordinate the use of the warriors that were available within the clans and tribes, and to coordinate their efforts towards a converging focal point that would be able to undermine the Russian traditional military superiority.

The author that really triggered the awareness about the new form of warfare, Hybrid Warfare, is Frank Hoffman. Looking at the conflicts in Afghanistan and Iraq, in which the U.S. was not only confronted by regular troops but also by local warlords, clans, members of the terroristic organisation Al Qaida and even armed drugs dealers, it became clear that the traditional concept of military thinking was no longer sufficient to face future wars. The US National Defense Strategy (NDS) 2005 recognised that new threats were arising and that, next to *traditional* threats, the US would also be confronted with *irregular*, *catastrophic* or *disruptive* threats[22]. The NDS defines these threats as distinguished categories, Hoffman assumes that future adversaries will not let themselves be put into one category, but will deploy more than one form simultaneously. "*The blurring of modes of war, the blurring of*

[19] William Nemeth, Future War and Chechnya: a Case for Hybrid Warfare, Naval Postgraduate School, June 2002.
[20] William Nemeth, Future War and Chechnya: a Case for Hybrid Warfare, Naval Postgraduate School, June 2002, p.4.
[21] William Nemeth, Future War and Chechnya: a Case for Hybrid Warfare, Naval Postgraduate School, June 2002, p.28-29.
[22] The National Defense Strategy of the United States of America, march 2005, retrieved from: http://www.space-library.com/0504nds2005.pdf

who fights, and what technologies are brought to bear, produces a wide range of variety and complexity that we call Hybrid Warfare[23]." He continues to assume that the efforts of all fighting parties, both state and non-state actors, (he calls them *multi-nodal activities)* are coordinated in order to achieve synergistic effects.

Hoffman considers the execution of the operations by Hezbollah during the war between Hezbollah and Israel in 2006, the be a clear example of contemporary Hybrid Warfare. Many well trained and disciplined cells were able to contest the modern, Western style organised, Israeli Defence Force (IDF) over territory, using a combination of guerrilla tactics and high-technology weaponry. Mingling with the civil population, as well as putting up fortifications nearby cities and villages effectively blurred who was fighting. At the same time a 'battle of perception' was fought. Through the extensive use of internet, the outside world was flooded with pictures and videos of the pain and suffering that was caused by the 'brutal and barbaric' operations of the IDF.

It is remarkable that Hoffman mentions this battle of perception, since his focus is primarily on the use of different forms of violence. Even in later publications he focuses on the adversary's modes of (violent) conflict and does not incorporate the use of information in order to influence both the enemy as the world opinion. As we will see later in this chapter, the use of information will become an essential element in other definitions of Hybrid Warfare.

In 2010 Hoffman refines his definition to read *''any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battlespace to obtain their political objectives*[24]*.''* Here a critical note can be placed. From a linguistic point of view Hoffman starts to make it confusing. In his 2007 article he already mixes up the terms War and Warfare, resulting in the situation were other scholars quote his description of Hybrid War when they try to explain what Hybrid Warfare is[25]. The above mentioned definition however, applies to what Hoffman describes as Hybrid Threats. According to the Cambridge dictionary a threat is: "a suggestion that

[23] Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies Arlington, Virginia December 2007, p.14.

[24] Frank G. Hoffman, 'Hybrid Threats': Neither Omnipotent Nor Unbeatable, July 2010, FPRI, p. 443. Retrieved from: https://www.fpri.org/article/2010/07/hybrid-threats-neither-omnipotent-unbeatable

[25] Jan Jakub Uzieblo, "United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats", EU Diplomacy Papers 5/2017, p. 6.; Kaspars Galkins, NATO and hybrid conflict: unresolved issues from the past or unresolvable threats of the present?, NAVAL POSTGRADUATE SCHOOL, September 2012, p. 10.

something unpleasant or violent will happen[26]", i.e. it is future oriented. This does not match the definition that is put in the present tense, suggesting that the adversary is already using one or more multi-nodal activities.

2.3 An intermezzo

A short intermezzo might be in order. The mix-up of terminology is seen throughout the whole discussion about Hybrid Warfare. Most articles deal with the topic addressed as "Hybrid Warfare". In these articles a mixture of terminology can be found. Some writers stick consistently to the term Hybrid Warfare, but many others use terms like Hybrid War, Hybrid Threat, Hybrid Conflict and even Hybrid Force[27], Hybrid Intervention[28] and Hybrid Challenges[29] throughout their papers. Hardly any of these writers clearly explains why they are using such a mixture of terms. Is it because they consider all those terms to be slightly different concepts and is the use of different terms intended to make a distinction, or is it just because they want to avoid using the same term over and over again and consider all the different terms to be synonyms, freely interchangeable?

Pawlak is one of the few who is very clear in his statement that there are differences between Hybrid Threat, Hybrid Conflict and Hybrid War. He sees Hybrid Threats as a complex and multidimensional threat, War and Conflict are considered to be ways for actors to achieve their goals. During a Conflict, (covert) military pressure and intimidation is used only in support of political, economic, diplomatic and technical means to pursue strategic objectives. When the adversary openly uses military force, as well as other means, he considers it to be War[30]. By using these definitions, whether they are fully correct or not, the author at least makes clear what his vision towards the subject is. When he uses a different term he actually does mean something different. This approach could be helpful in the discussion over a subject that is so complex by nature and does not need extra confusion caused by linguistics.

[26] Definition of "threat" from the Cambridge Advanced Learner's Dictionary & Thesaurus.

[27] Timothy B. McCulloh, The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?, JSOU Report 13-4, The JSOU Press MacDill Air Force Base, Florida 2013, p. 2.

[28] Margriet Drent et al, New Threats, New EU and NATO Responses, Netherlands Institute of International Relations Clingendael, July 2015, p.10.

[29] Craișor-Constantin IONIȚĂ, Is hybrid warfare something new?, Strategic Impact No. 4/2014, p. 63.

[30] Patryk Pawlak, Understanding hybrid threats, European Parliamentary Research Service Blog, https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/

2.4 HYBRID ONLY FOR THE UNDERDOG?

To return to the concept, both Hoffman and Nemeth, both former officers in the US Military, consider Hybrid Warfare as the open use of a mixture of forms of violence, used by a weaker opponent against a strong, modern force in order to get the upper hand in a conflict over a defined geographical area. As early as 2007 another US Army officer, Col. Margaret Bond, takes a different approach to Hybrid War. She states that future wars will be about projecting all elements of national power, including a broad spectrum of military activities, but also applying economic and political pressure in order to change conditions in failing states[31]. Acknowledging that stability operations will be one of the core activities of the US Military, and that the traditional approach in which the military will only do the fighting, and will hand off the development and reconstruction activities to other agencies, does not turn out to be effective, she calls for more involvement of the US Military in stabilisation operations. "To be effective in implementing US national policy for stabilizing failing states and resisting the flow of terrorist groups or insurgencies into ungoverned spaces, hybrid war must take place well before the indigenous government fails and the initiative for stability is lost. In short, to be effective for security stabilization, Hybrid War needs to be implemented early in the continuum of US involvement in 'at risk' states, and hybrid warriors, with their shovels and weapons, deployed well before hostilities occur[32]." Unlike Nemeth and Hoffman, Bond considers Hybrid Warfare as a phenomenon not only employed by weaker, less organised advisories, but it will also be used by the strong, well organised states like the US.

2.5 ADDING MORE ASPECTS TO THE CONCEPT

Realising that the future security and defence challenges to the alliance were changing, also NATO picked up the concept of Hybrid Threats. In 2009 NATO Allied Command Transformation (ACT) released a report called 'Multiple Futures Project, navigating towards 2030' (MFP). In this report ACT predict that Hybrid Attacks will target NATO's fundamental principles, and adversaries will attack NATO's populations, centres of commerce, and the integrated global economy[33]. Unlike authors like Nemeth and Hoffman, NATO assumes that not only forces that operate abroad will be attacked, but also the populations of NATO

[31] Colonel Margaret S. Bond, Hybrid war: a new paradigm for stability operations in failing states, U.S. Army War College, 30 Mar 2007, p. 4.

[32] Colonel Margaret S. Bond, Hybrid war: a new paradigm for stability operations in failing states, U.S. Army War College, 30 Mar 2007, p. 11.

[33] NATO ACT, Multiple Futures Project, navigating towards 2030, April 2009, p. 7. www.act.nato.int/nato-multiple-futures-project-documents

member states will become targets for opposing actors. Thus bringing the threat much closer to home. The attackers would combine traditional and irregular warfare, terrorism, and organised crime, as well as mass media to undermine the western values. To make it even more complex, Hybrid adversaries will seek to use the Western civil norms, their commitment to the rule of law and the freedom of speech and media against the Alliance[34].

In response to the MFP, the NATO Bi-Strategic Commands (Bi-SC) came up with an concept for the NATO Military Contribution to Countering Hybrid Threats (MCCHT). The definition used in the MCCHT is very concise: "*Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives*[35]". Next to this definition a context is given, in which NATO explains that adversaries, both state and non-state actors, will apply pressure across the entire spectrum of conflict, using economic/financial, legal, political, social and military/security means[36]. Rather than digging further into the definition of Hybrid Threat, the Bi-SC input focusses on measures that have to be taken by the Alliance in order to counter these threats. It is noticed that a military solution by itself will not be sufficient to counter Hybrid Threats and that a comprehensive approach is necessary. This approach should include broader political, military and economic incentives, as well as a different approach towards partnerships[37]. While the MFP is warning that adversaries will attack 'our populations', the MCCHT does not address this threat. On the contrary, a statement like "The Alliance could be portrayed as a foreign intervention force[38]" does suggest that Hybrid Warfare will omly be conducted against NATO forces that are physically inside a foreign country.

2.6 Hybrid War and Russia

In 2013 the Russian Chief of Staff, general Gerasimov, fuelled the discussion about Hybrid Warfare even more. In an article, published in a private newspaper that is frequently used by military leaders to inform the forces, Gerasimov explains his view on past, present and future

[34] NATO ACT, Multiple Futures Project, navigating towards 2030, April 2009, p. 7.

[35] BI-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats, 1500/CPPCAM/FCR/10-270038 5000 FXX 0100/TT-6051/Ser: NU0040, August 2010, p.2. www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

[36] BI-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats, 1500/CPPCAM/FCR/10-270038 5000 FXX 0100/TT-6051/Ser: NU0040, August 2010, p.2-3.

[37] BI-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats, 1500/CPPCAM/FCR/10-270038 5000 FXX 0100/TT-6051/Ser: NU0040, August 2010, p.5-6.

[38] BI-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats, 1500/CPPCAM/FCR/10-270038 5000 FXX 0100/TT-6051/Ser: NU0040, August 2010, p.4.

warfare[39]. In the article Gerasimov describes that by using a variety of non-military means such as political, economic, informational, humanitarian measures in combination with the protest of the people, a (relative) stable state can be turned into chaos, dragged into a civil war and become target for a foreign military intervention. He signals that the division between war and peace is fading and that the rules of war have changed. The use of traditional forces to win the battle is reduced. Rather the use of concealed force is chosen, supported by non-military measures like no-fly zones, sea blockades, and the deployment of private military companies[40].

Both Bartles and Coalson indicate that Gerasimov is giving a description of what he thinks the West is doing, and stress that is **not** the revelation of a new Russian doctrine. It is more a call for military scientists to observe what is going on in the world and to start thinking about new ways of employing force and to look for the enemies vulnerabilities and ways to overcome these. Coalson indicates that the article merely shows the way Russia is looking at the West, and in particular to the US. Galeotti states that when he introduced the term ‘Gerasimov doctrine’, he was just searching for a “snappy title” and he never expected the term to be broadly used. He himself does not consider Gerasimov’s view to be a doctrine, only his interpretation of what is going on in the world[41].

But the events in Ukraine in 2014 triggered a lot of scholars to see, in retrospect, the Gerasimov article as an actual forecast of the intentions of Russia. Popescu concludes that the Russian intervention in the Crimea “followed a script very much in line with Gerasimov’s doctrine[42]”. Samadashvili is even more convinced that the article is an actual doctrine. According to her, the article indicates how **Russia** can intervene in others states without an open conflict; that the use of political, economic, informational, humanitarian and other non-military measures is promoted by Gerasimov in order to overthrow a foreign regime[43]. She directly links the term to Russia, and does not treat it as a general concept that can be used by anyone.

[39] Charles K. Bartles, Getting Gerasimov Right, Military Review, Jan-Feb 2016, p. 30-31.

[40] Robert Coalson, Top Russian General Lays Bare Putin’s Plan for Ukraine, Huffpost, Sept 2014. https://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html

[41] Mark Galeotti, The ‘Gerasimov Doctrine’ and Russian Non-Linear War, In Moscow’s shadows, July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

[42] Nicu Popescu, Hybrid tactics: Russia and the West, European Union institute for Security Studies, October 2015, p. 1.

[43] Salome Samadashvili, Muzzling the Bear, Strategic Defence for Russia’s Undeclared Information War on Europe, Wilfried Martens Centre for European studies, 2014, p.17.

It is not the intention in this chapter to come up with a judgement who is wrong and who is right, but it is safe to say that scholars have fundamentally contrasting notions on how to interpret Gerasimov's article; Is it a description of an unfriendly outside world that is threatening Russia, or is it a master plan for Russia to regain dominance in strategically important areas?

Without going into the details, it is appropriate to highlight certain hybrid measures used by the Russians during the annexation of the Crimea. These measures convinced many Western scholars that Russia was using the Gerasimov Doctrine to deliberately employ Hybrid Warfare in order to reach strategic goals.

Bartovski gives a clear description of the Russian use of information (and disinformation) in order to influence their adversaries, to mobilise the Russian minority living in the Donbas area, to divide the Western allies and to keep the Russian population in the dark. He also points out that the Russians were offering financial and institutional incentives to Ukrainian soldiers in order to defect, or at least not to intervene, as well as to governmental agencies. The Russians also sent in humanitarian convoys, without any clearance or approval from the Ukrainian government. Although it was suspected that the convoys would be carrying weapons for the separatists, the Ukrainian government did not dare to intervene with this convoys. Unjustifiable attacking clearly marked humanitarian aid, might have given the Russians all the reason to openly intervene in the conflict. All in all, a large part of the Ukrainian military did not engage in any form of combat, allowing the 'little green man', unknown (but generally assumed to be Russian) fighters who dressed in unmarked green uniforms and were wearing their small arms openly, to take possession of key positions in the area[44].

Weitz states that "the Russian government's Ukraine-campaign highlighted how Moscow orchestrates strategic communication, psychological operations, psychological pressure, economic threats, and sub-military force as well as conventional military power." He continues by describing 10 categories of action, taken by the Russians, varying from information and propaganda, to economic measures (both positive and negative), cyberattacks and the mobilisation of ethnic Russians. He also points out that the Russians deployed military units to the border region, not only to intimidate the Ukrainian government, but also

[44] Maciej Bartkowski, Nonviolent Civilian Defense to Counter Russian Hybrid Warfare, The Johns Hopkins University Center for Advanced Governmental Studies, March 2015, p.8-10.

to provide mental support to the separatists and to scare off any foreign power that might be willing to help the Ukrainian government with military means[45]. Russia did already have some 15,000 troops in the area since it had an agreement with the Ukrainian government that they could maintain to operate the Black Sea Fleet from the Crimea. This military presence, as well as the fact that the majority of the Crimean population consists of ethnic Russians, made preparations for the use of force by Russia, both overt and covert, relatively simple[46].

Overall the Russian operation to annex the Crimea clearly showed the coordinated use of all elements of state power (diplomacy, information, military, and economy[47]) in order to achieve their goals. The techniques used by Russia, and the elements of state power deployed, were clearly linked to each other and mutually reinforcing[48]. These elements of state power however, and the use of them in an attempt to achieve strategical goals, are not new. They are already described by Kenan in 1948 when he introduced the concept of political warfare as "*the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP--the Marshall Plan), and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states*[49]". This basically brings us back to Gerasimov; was the Ukraine operation the first try-out of a new doctrine, or did the Russians simply copy a well-known American form of warfare?

2.7 EVEN MORE HOLISTIC

In 2016 Cullen and Reichborn-Kjennerud added a new chapter to the discussion. They describe that "*HW is characterized by the tailored use of all instruments of power against the vulnerabilities of the opponent's system*[50]." These instruments of power are Military, Political,

[45] Richard Weitz, Countering Russia's Hybrid Threats, Diplomaatia No. 135 • November 2014, https://www.diplomaatia.ee/en/article/countering-russias-hybrid-threats/

[46] Michael Cecire, The Russian invasion of Ukraine, Foreign Policy Research Institute, March 2014, https://www.fpri.org/docs/cecire_crimea.pdf

[47] Margriet Drent et al, New Threats, New EU and NATO Responses, Netherlands Institute of International Relations Clingendael, July 2015, p.29.

[48] Katie Abbott, Understanding and Countering Hybrid Warfare: Next Steps for the North Atlantic Treaty Organization, University of Ottawa, March 23, 2016, p. 10.

[49] George Kenan, The inauguration of organized political warfare, Policy Planning Staff Memorandum, May 1948, http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm

[50] Patrick J. Cullen and Erik Reichborn-Kjennerud, Countering Hybrid Warfare (CHW); Baseline Assessment, Multinational Capability Development Campaign (MCDC), October 2016, p. 17.

Economic, Civilian and Informational (MPECI) and these will be used to target an adversaries weaknesses in the Political, Military, Economic, Societal, Informational and Infrastructure (PMESII) domain.

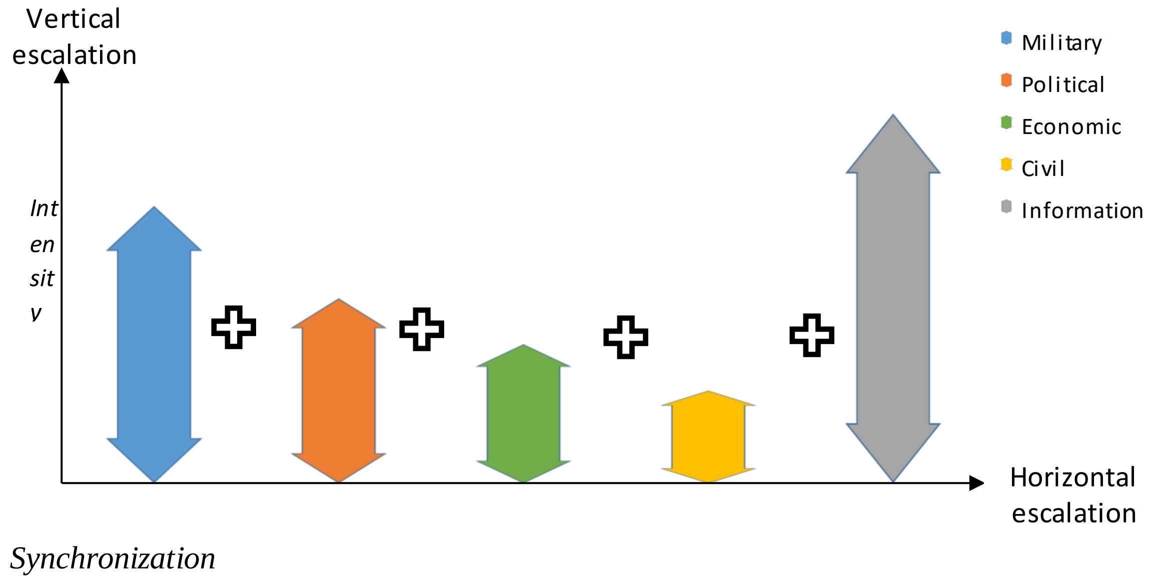


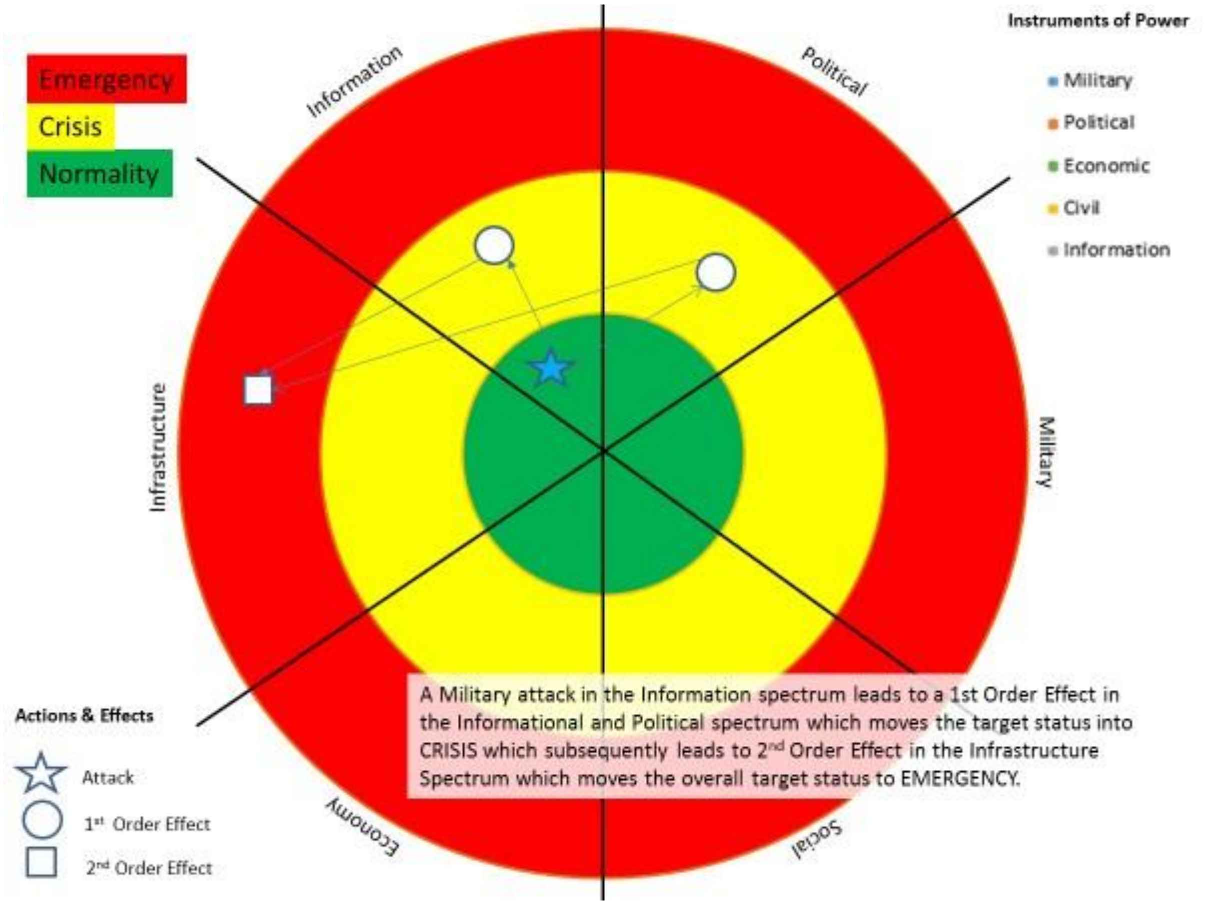
Figure 1: The Horizontal and Vertical Escalation of the instruments of power[51]

Figure 1 shows the synchronisation between the instruments of power in time, space and purpose. Maximum effect is achieved by a coordinated and tailored use of the instruments. In different stages of the conflict different instruments should get priority. In the given illustration a lot of effort is put into Information activities, backed up by military activities. Political, economic and civil measures are less deployed. The ability to synchronize both military and non-military means simultaneously within the same battlespace is considered to be an essential aspect of Hybrid Warfare[52]. But in order to be able to coordinate all the elements of power, a high degree of centralised Command and Control over both state and non-state elements is mandatory. It is the authors opinion that it is therefore not likely that Hybrid Warfare as described by Cullen and Reichborn-Kjennerud can be executed by non-state actors like ISIS, nor by democratic actors. Neither of those has sufficient control over all elements of power.

[51] Patrick J. Cullen and Erik Reichborn-Kjennerud, Countering Hybrid Warfare (CHW); Baseline Assessment, Multinational Capability Development Campaign (MCDC), October 2016, p. 17.

[52] Patrick J. Cullen and Erik Reichborn-Kjennerud, Countering Hybrid Warfare (CHW); Analytical Framework, Multinational Capability Development Campaign (MCDC), October 2016, p. 11.

The use of a broad set of elements of power creates surprise and triggers psychological effects that masks the ones that are really trying to achieve their goals. This masking connects with an older British term called Ambiguous Warfare: “hostile actions that are difficult for a state to identify, attribute or publicly define as coercive uses of force.” As in Ambiguous Warfare, Hybrid Warfare aims at disrupting the decision making processes of an adversary, and to prevent that adversary to attribute actions to the aggressor. Without being able to proof who the actual aggressor is, it is almost impossible to employ military measures in a legitimate way, or to mobilize international support to counter the aggressor. “The prosecution and countering of Ambiguous Warfare looks like neither war nor peace, erasing this important dichotomy and moving into the grey areas of conflict.[53]”



A Military attack in the Information spectrum leads to a 1st Order Effect in the Informational and Political spectrum which moves the target status into CRISIS which subsequently leads to 2nd Order Effect in the Infrastructure Spectrum which moves the overall target status to EMERGENCY.

Figure 2: Visualizing HW [54]

[53] Patrick J. Cullen and Erik Reichborn-Kjennerud, Countering Hybrid Warfare (CHW); Baseline Assessment, Multinational Capability Development Campaign (MCDC), October 2016, p. 9.

[54] Patrick J. Cullen and Erik Reichborn-Kjennerud, Countering Hybrid Warfare (CHW); Analytical Framework, Multinational Capability Development Campaign (MCDC), October 2016, p. 13.

Figure 2 illustrates a planned use of one instrument of power in the PMESII domain. The planned military action in the information domain has a first order effect in both the Information and the Political spectrum. But it also has a second order effect. This second order effect might reinforce the intended effect, but it can also be counterproductive. For example, if the Russians would have targeted the internet in the Crimea in order to prevent the Ukrainian government to broadcast the Russian intervention to the world, it would also cut-off the ethnic Russians from the internet. If then the only remaining means of information would have been the Ukrainian state television, they could be influenced in such a way that they would stop supporting the Russian action. The problem with non-linear second -and even third- order effects, is that they are hard to predict and are mostly only observed after they have occurred[55]. This has serious effect on the usefulness of Hybrid Warfare. Decisionmakers should be aware that even carefully planned actions might have effects that backfire on them.

2.8 EU AND HYBRID

One major contributor to the discussion on what Hybrid Warfare is missing in this chapter: the EU. The EU also came up with an vision on the concept, but since the EU description of Hybrid Warfare is used as the starting point for this thesis, it will be covered more in depth in chapter 5. For now I will just quote the description as issued in 2015[56]. According to the EU, Hybrid Warfare can be characterised as a centrally designed and controlled use of various covert and overt tactics, enacted by military and/or non-military means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces, in order to undermine and destabilise an opponent[57]. This description of the concept does not require a highly sophisticated Command and Control organisation and extensive control of all elements of state power. Therefor the EU does not only consider regular states like Russia and China as entities that might deploy Hybrid Warfare against others, but the definition also can be, and is, applied to organisations like ISIS and even 'the current government in Turkey'[58].

[55] Patrick J. Cullen and Erik Reichborn-Kjennerud, Countering Hybrid Warfare (CHW); Analytical Framework, Multinational Capability Development Campaign (MCDC), October 2016, p. 13.

[56] Since this chapter is about the concept and its development, the initial description of the concept is chosen. Further details can be found in chapter 5.

[57] EEAS(2015) 731, Food-for-thought paper "Countering Hybrid Threats", European External Action Service, May 2015, p. 2.

[58] Patryk Pawlak, Countering hybrid threats: EU-NATO cooperation, European Parliamentary Research Service, March 2017, p.2.

2.9 SUMMARY OF THE EVOLUTION OF HYBRID WARFARE

In this chapter we have seen the development of the concept of Hybrid Warfare. It started off as a smart way for relatively weak states to combine and coordinate available fighting capacity, regular military, irregular troops, terrorists and organized crime, in such a way that they could defend themselves against a much stronger opponent that had invaded their country. In a period of just fourteen years it has transformed into an all-inclusive way of warfighting, strictly orchestrated by a strong central agency (or: an authoritarian but stable political authority[59]), which has control over all elements of state power. Hybrid Warfare is no longer only viewed as a defensive way of operation, it is nowadays also considered to be an effective way to perform offensive operations against other nations and to expand ones territory. Not only are foreign troops -deployed in other countries- targets for Hybrid Warfare, also the home-population of Western nations can be targeted. Some even go as far as claiming that NATO member states such as the Baltic States might be at a point where their territorial integrity is being challenged by Russia, using Hybrid Attacks to achieve Russian goals[60]. Although certain aspects of the initial description of Hybrid Warfare by Nemeth are still valid, i.e. the use of different forms of force, the blurring of who is fighting, the use of information and mass media to influence both own and external population, the concept has changed from a simple defensive form of warfare towards a highly complex and versatile way of operating, demanding a high level of command and control. In a bracket of only 14 years the concept has undergone a tremendous change, and it has become much more frightening than it was when it was first mentioned by Nemeth.

[59] Can Kaspoglu, Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control, NATO research paper 121, November 2015, p. 12.

[60] Henrik Praks, Hybrid or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics The Case of Estonia, in: Guillaume Lasconjarias and Jeffrey A. Larsen, NATO's Response to Hybrid Threats, NATO Defense College, Forum Paper 24, 2015, p.220-221.; David Takacs, Ukraine's deterrence failure: Lessons for the Baltic States, Journal on Baltic Security, 2017; 3(1): 1–10, p.1.

3 HYBRID WARFARE, A TRULY NEW AND SCARY PHENOMENON?

"No-one should be under any illusion but that the threat posed by hybrid warfare is real[61]*"*

3.1 HYBRID WARFARE AND REALISM

Not all scholars see Hybrid Warfare as a new terrifying monster. It is not that they do not recognise the threats that are depicted by the advocates of the concept Hybrid Warfare. It is more that they don't think that it is anything new, or that Hybrid Warfare is extra complicated compared to the conflicts humanity has already seen. Almost 200 years ago, von Clausewitz already stated that "although war changes its characteristics in various circumstances, in whatever way it manifests itself, war is still war.[62]" War has always been a complex set of interconnected actions that served political goals. According to van Puyvelde, wars are usually shaped through the asymmetric exploitation of the weaknesses of the adversary. He wonders whether Hybrid War even exists and advices decision-makers to focus on the threats they are confronted with, and to look for connections between these threats and to forget all about Hybrid Warfare[63].

Biscop is writing about Hybrid Hysteria. When looking at the Russian attempts to influence EU member states, to acquire critical infrastructure in other countries, to financially support weak governments, to create political unrest and to turn the population against its government, to instrumentalise the energy market, many scholars come to the conclusion that Russia is already waging Hybrid War against the West. This, according to Biscop, is not true. Annoying and obstructing other states are normal instruments of statecraft. As a matter of fact, the West is using the same instruments of statecraft to bring peace and prosperity to weak or failed states. But if the West is doing so, it is called the Comprehensive Approach.

Biscop goes as far as describing Hybrid War as "the Comprehensive Approach gone over to the dark side", indicating that the means are similar, only the intentions differ: Western intentions are good, all others have bad intentions….. The usability of Hybrid Warfare as a way to achieve Russian strategic goals is, according to him, very limited. In Ukraine it might have worked, but this was almost a domestic quarrel for the Russians, and the circumstances

[61] European Parliament, EPP Group, The supreme art of war is to subdue the enemy without fighting, Brussels, 19 April 2016.
[62] Quoted from Mary Ellen O'Connell, Myths of Hybrid Warfare, in Ethics and Armed Forces, Issue 2015/2, p.27.
[63] Damien van Puyvelde, Hybrid War – does it even exist? NATO review magazine, 2016. https://www.nato.int/docu/review/2015/also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm

were ideal. The EU states are stable and wealthy democracies in which the rule of law, human rights and personal freedom are critical values. It is very unlikely that Russia will succeed in turning the population against its government, what better narrative could they have to offer? In order to create disturbance amongst the people two elements are required: a group of dedicated individuals who prepare the information and take care of the dissemination, and there must be a set of dormant grievances and other motivations that can be triggered[64]. The mobilisation of the ethnic Russians in the Crimea was successful and turned out to be a critical enabler for the success of the covert operations. But what are the chances that Russia will be able to mobilise substantial groups in Western societies for their course, and give them the advantage they need to achieve their goals?

Of course the threat from external influencing should not be downplayed and the EU should reduce its vulnerability, invest in cybersecurity, secure the critical infrastructure, and explore more energy sources in order to reduce our dependency on a few suppliers. Another spearpoint should be the fighting of corruption, and making sure that citizens and government treat each other with respect and that no members of society are excluded. With the proper preparations Hybrid Warfare is not worth creating panic, “Alarmism is not just unnecessary; it is also singularly unhelpful[65].”

Charap notices similar things when looking at NATO. The Russian operation in Ukraine did reveal that Moscow was able to coordinate all elements of state power in order to achieve its goals, thus fitting the definition Hybrid Warfare. The Ukrainian operation was conducted in near perfect conditions. As a remnant of the Soviet era, a large Russian ethnic majority populated the Crimea, Russia still had military bases in the area, intelligence networks were present, the Ukrainian government was weak after the Maidan revolution. In this permissive environment the Russian efforts were successful. Successful for the limited goals Russia had; it was only concerned about the Crimea because of the economic and military interests they had in that region.

Based on these successful actions, some Western analysts concluded that Russia has a ready-to-use Hybrid doctrine, that can be applied against NATO members as well. Countries like Estonia and Latvia, who also were part of the Soviet Union and given their sizeable Russian-

[64] Ignas Kalpokas, Influence Operations: Challenging the Social Media – Democracy Nexus, Sais Europe journal of global affairs Volume 19, p. 18.

[65] Sven Biscop, Hybrid Hysteria, Security Policy Brief no. 64, June 2015, pp.1-4. http://www.egmontinstitute.be/content/uploads/2015/06/SPB64.pdf?type=pdf

speaking, non-citizen minorities, are considered to be possible targets. Based on the various diplomatic, economic, military and subversive measures that have been employed by Russia in the Baltic Region, some analysts claim that Russia is already conducting Hybrid Warfare against NATO. But that conclusion is, according to Charap, a dangerous way to misuse the word 'War'. Like Biscop, Charap sees the measures that are deployed by Russia as normal instruments of statecraft. On top of that, he claims that in case Russia would have the intention to violate the territory of the Baltic States this would result in traditional war with NATO. And that is something Russia cannot afford.

Another remarkable statement Charap makes, is that East and West are pointing fingers at each other, over what is basically exactly the same behaviour. The West sees the Russian actions in Ukraine as *the* proof for their bad intentions, while Russia claims that the Maidan revolution, that proceeded the Russian actions, was a typical Western demonstration how to orchestrate a regime change, using all kind of measures short of the open use of force. And like NATO, Russia is paranoid. They too belief that, because NATO is able to provoke a regime change in their backyard, they will be able to do so in Russia as well. And that the West will make use of every opportunity to do it. Although the fear for the other can be understood, Charap claims that the assessment of the others intentions and capabilities are highly exaggerated[66].

3.2 HYBRID WARFARE AS VEHICLE TO CREATE OWN POSSIBILITIES

Tenenbaum suggests that the concept of Hybrid Warfare has been misused in discussions of a completely different order to get priority and budget for security matters. Think-tanks, individual EU and NATO member states and centres of excellence, all used the concept to get their perspective on to the agenda. This seems a logical statement, considering the fact that all governmental agencies were confronted with budget cuts since the beginning of the financial crisis in 2008. The defence and security branches were not excluded from these cuts. For example, the Dutch military budget was reduced by 12% in 2010. Under these budgetary discussions, the meaning of the originally sound concept of Hybrid Warfare "has been diluted to the point of absurdity", according to Tenenbaum. The concept was stretched from a mixture between regular and irregular warfare to a concept that now includes cyberwar, organized crime, propaganda, or economic warfare, or in other words: it now describes the overall complexity of modern-day conflicts. It is the irregular part of warfare that worries the

[66] Samuel Charap, The Ghost of Hybrid War, Survival, vol. 57 no. 6, December 2015–January 2016, pp. 51–58.

West. Regular warfare is focussed on defeating the enemies forces, the West is extremely good at that, depending on superior high-tech weaponry. Irregular strategy, using psychological operations, social and economic activities, subversion or even terrorism, is used to slowly erode the enemy's willpower and the control over its population and does not adhere to the predictable rules of regular warfare[67].

The West has invested a lot of effort in the last few centuries in organising society and warfare. Political order depends on a clear distinction between war and peace. Peace is the preferred order since it is needed to achieve economic growth and prosperity. War is sometimes necessary to settle disputes, but should be executed on behalf of the state, fought by specialists and adhere to all sort of rules. By institutionalising peace and war as acts of law (declaration of war and peace agreement), a binary order was created. There was either war or peace, there was no in-between. According to Münkler, Hybrid War is all about occupying that in-between. The terms only use is to describe the phenomenon that nowadays all kind of actors, both state and non-state, can disturb political order by a variety of measures which do not cross the line of war, but certainly undermine our feeling of peace. Since the term Hybrid Warfare is an all-inclusive term without discriminatory force, it has no ordering or prescriptive dimension[68].

The United Nations Charter prohibiting states to reach for to military force was ratified in 1945 and is still in force. This Charter also assumes a binary order, it is either war or peace. And only in war it is allowed to use military force. What is, and what is not allowed during war is recorded in international law principles. Using psychological operations, social and economic activities, subversion or even terrorism, state and non-state actors can seriously undermine ones security without crossing the line of an official war. This makes it for a nation hard protect itself against such actions. After all, since there is no war going on, the options for "biting back" are very limited. The principles of *jus ad bello* and *jus in bello* cannot be easily applied. The jus ad bellum criteria are concerned with how to justify going to war,

[67] Élie Tenenbaum, Hybrid Warfare in the Strategic Spectrum: An Historical Assessment, in Guillaume Lasconjarias and Jeffrey A. Larsen, NATO's Response to Hybrid Threats, NATO Defense College Forum Paper 24, pp. 95-112.

[68] Herfried Münkler, Hybrid Wars. The Dissolution of the Binary Order of War and Peace, and Its Consequences, Ethics and Armed Forces, Issue 2015/2, pp. 20-23.

while the jus in bello criteria are dealing with what may be done during war, and against whom[69].

O'Connel states that the term Hybrid War was introduced to open up the possibility to respond with military force to such actions, without violating international law. By calling them warfare, the normal instruments of statecraft are made so threatening that they justify a response by force. The US even considers "economic aid" to be a Hybrid Threat. Doing so gives the impression that economic aid is illegal, and limits the right for other nations to help states economically.

To O'Connel, Hybrid War can only be considered to be war when actual fighting is involved. Things like economic aid and cyber activities can be part of Hybrid Warfare, but do not qualify as such by themselves. Of course unlawful cyber activities like spying, theft, and property damage are executed by state and non-state actors, but these activities are already illegal by national or international law. They are therefor just criminal acts. Something that can be classified as cyberwar has not yet occurred, O'Connel claims[70]. When a state has been the victim of cyber activities, international law contains means of responding lawfully, including with coercive means, there is no need to call it war to provide proper means to respond.

3.3 HYBRID WARFARE AND CYBER

To go a little deeper into cyber activities, which is one of the most elusive threats from the concept of Hybrid Warfare, Gill and Ducheine do not rule out the possibility of a cyberattack that can actually be classified as and armed attack under the contemporary international legal framework. Cyberspace is not treated different in international law than the physical world. Therefore, notions such as "use of force," "armed attack," "necessity," "immediacy" and "proportionality" are valid and have to be adhered to. According to the authors "an armed attack could arguably include a cyber-attack directed against a State's critical infrastructure, provided the cyber-attack had the potential to severely cripple a State's ability to carry out and ensure the conducting of essential State functions or severely undermine its economic, political and social stability for a prolonged period of time."

[69] David Whetham, "Hybrid Warfare" and the Continuing Relevance of the Just War Tradition in the 21st Century, Ethics and Armed Forces, Issue 2015/2, p. 33.

[70] Mary Ellen O'Connell, Myths of Hybrid Warfare, in Ethics and Armed Forces, Issue 2015/2, pp.27-30.

So, under specific conditions, it is possible to classify cyberactivity as a hostile act. In such a situation the use of force to react could be justified. But hardly any of the cyberattacks, as reported in the media, have shown the use of force. And they definitely did not meet the criteria for an armed attack. The denial-of-service "attack" on Estonia in 2007, which resulted in a few hours of disruption and inconvenience, was disruptive and illegal, but could not be classified as an armed attack, nor can the numerous examples of cyber break-ins, espionage, sabotage and theft of data and intellectual property. Not even the use of the Stuxnet virus, that caused some physical damage and delayed the Iranian nuclear program, did qualify as an armed attack, and thus as an act of war. Gill and Ducheine do not qualify the Iranian nuclear program as essential for the proper functioning of the state, since fossil fuels (86.1%) and hydroelectric plants (13.7%) provide for most of Iranian energy demand.

Cyber espionage, cyber sabotage and cyber-criminal activity aimed at both public and private computer systems can be observed on an almost daily basis. These constitute serious threats to a state's national and economic security, but they do not constitute armed attacks. The authors don't think that it is very likely that a standalone armed cyberattack will occur since an attack on that scale would inevitably trigger a large-scale kinetic response. To them it is more likely that an attack will be launched in which cyber capabilities are used, alongside traditional kinetic armed force, as a means of "preparing the battlefield," thereby creating favourable circumstances for the overall success of the operation[71]. Based on Gill and Ducheine, one can conclude that authors that claim that ongoing cyber activities are part of a Hybrid Warfare campaign that is already in progress are, as we saw Charap stating a little earlier in this chapter, dangerously misusing the word war.

3.4 STAY CALM, DESPITE THE THREAT

None of the authors in this chapter denies the threats towards our security that we are facing nowadays. Psychological operations, social and economic activities, cyber, and subversion conducted by both state and non-state actors can be, and sometimes are, deployed against Western democracies. These activities are annoying, do influence public opinion in a negative way, might be illegal, might limit the growth of our economies, double-cross our political and economic interests, but they do not qualify as war under the international legal framework. As a matter of fact, it is part of normal politics. Calling these activities Hybrid Warfare, and

[71] Terry D. Gill and Paul A. L. Ducheine, Anticipatory Self-Defense in the Cyber Context, International Law Studies, 2013, pp. 438-463.

claiming that it is already conducted against us, seems to have served one major cause: it helped to get defence and security issues back on the agenda; threats are all around and us and these threats are so serious that the use of force is justified. Again, no one denies the existence of the threats, nor the fact that these threats can have devastating effects on societies, calling them war is however not the correct response. One can invest in prevention, one can counteract in accordance with contemporary international law, but "especially in these times, it is important not to stir up fear"[72].

[72] Gertrud Vaske, Hybrid Warfare – A Crisis on Our Doorstep, in Ethics and Armed Forces, Issue 2015/2, p. 42.

4 METHODOLOGY

4.1 INTRODUCTION

In this chapter the methodological choices for this research will be explained. The first part will cover definition of the concept of Hybrid Threat. Next the research design and explain why a qualitative single case study the suitable design is for this research. The next paragraphs will contain the operationalisation of the design into indicators, the data collection and the way of analysis. The final part will reflect the limitations of this study.

4.2 DEFINITION

The first step in this research will be the exploration of the policy on Hybrid Threat as advocated by the EU. As mentioned before, many different definitions can be found that cover this concept. Even though many different definitions exist, and the concept is still under development, the definition used by the EU will be the baseline. This provides clear boundaries for the concept and avoids ambiguity over the elements that are, and are not, included in the definition. The EU states that in general the concept of Hybrid Threats "*aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare*[73] ".

4.3 RESEARCH DESIGN

The development of policies and the implementation of it cannot be measured in a quantitative way. So to answer the research question a qualitative case-study approach will be used.

Qualitative research aims to understand, explain, explore, discover and clarify situations, feelings, perceptions, attitudes, values, beliefs and experiences of a group of people. Qualitative study designs are flexible and emergent in nature, as is the method of data collection[74]. A case study is an empirical inquiry within its real-life context that allows for deep examination of a phenomenon[75], and this study is about in-depth examination. The EU is

[73] A full explanation of the concept will be given in chapter 5.2.

[74] RanjitKumar, research methodology a step-by-step guide for beginners 3rd edition, SAGE Publications Ltd, 2011, p. 103-104.

[75] Robert K. Yin, Case Study Research, 3rd edition, Applied social research methods series Vol 5, Sage publications, 2003, pp. 1-7.

a large and complex organisation and cannot be studied as a whole in a Master thesis, so a single case has been chosen. In this study the influence of the EU initiatives on the development of the Dutch approach towards Hybrid Threats will be examined.

The case selection has been on relative simple grounds: being a Dutch citizen and being involved in the Dutch defence and security branch myself, I do have knowledge of the system and I have access to certain governmental agencies. This did not only give me direct access to information, but was also beneficial in the efforts to expand the network and get in contact with other relevant actors. Last but not least, reading and speaking in your native language makes it easier to understand subtle nuances in written documents and spoken statements.

4.4 Operationalisation

The EU has picked up the phenomenon of Hybrid Threats and has come up with a policy and has established several agencies and structures in order to facilitate member states to counter these threats. Member states are responsible for their own defence against Hybrid Threats[76] and have to develop their own policies and means to do so. Aligning the national efforts with the EU policy will require activities by the Netherlands.

The first thing is to look at is whether the EU view on Hybrid Threats is shared by the Netherlands, if so, the Netherlands should have (or should be working on) an own national policy on Hybrid Threats. If the threats are taken seriously, some indicators should be found during this research:

- a policy to counter the threats; countering Hybrid takes involves a lot of stakeholders, both public and private. It is impossible to steer all these stakeholders in the same direction if there isn't an overarching document that lays out the gaols end objectives that should be pursued.
- budgets, since these are essential to allot people and resources. If there is no money dedicated to Hybrid, it is impossible to achieve substantial results. All efforts in the field of Hybrid would have to compete for time and resources with existing policies and initiatives. This would lead to only very limited capacity to deal with Hybrid.
- dedicated organisational elements that are (fulltime) working on the subject; Only dedicated personnel will be able to acquire sufficient expertise and make it possible to establish networks to coordinate the efforts. Treating Hybrid as a secondary job

[76] This will be explained in chapter 5.2.

would lead to an expulsion effect in which staff members constantly have to chose between putting effort in existing, proven policies and investing time in the new kid on the block.

- coordination structures that aim to expand the network of players and share knowledge and information; Even if there are budgets assigned and organisational elements are established, it still requires coordination structures to bring the relevant players together. These structures should be institutionalised in order to make sure that the right actors share the right information at the right time.

If the EU initiatives are considered to be meaningful, the research should show that the Netherlands is trying to align their efforts with the EU approach. This would mean that Dutch national activities are aiming to finetune EU initiatives to fit the Dutch situation, rather than developing a completely different approach. Also the participation in EU established organisational elements and coordination structures can be seen as prove that the Netherlands sees these initiatives as meaningful.

The indicators that will be used to show that the EU initiatives on countering Hybrid Threats has influenced The Netherlands the Dutch approach are:

- The concept of Hybrid Threats is incorporated in policy documents,
- Budgets are assigned to counter Hybrid Threats,
- National or international organisational elements dealing with Hybrid Threats are (being) established,
- National or international coordination structures on Hybrid Threats are (being) established.

Since it is not yet clear whether the Netherlands is convinced that Hybrid Threats are real threats that should be countered, first will investigated whether an indicator can be found, and if so, to what extend the content of that indicator aligns with the EU initiatives.

4.5 DATA COLLECTION

In order to find the indicators, a retrospective document analysis on policy papers and governmental documents of the three most important ministries that are dealing with Hybrid Threats will be performed. These ministries are:

- Justitie en Veiligheid[77] (JenV). The Ministry of Justice and Security ensures the rule of law in the Netherlands, so that people can live together in freedom, regardless of their lifestyle or views. Justice and Security works towards a safer and more just society by giving people legal protection and intervening where necessary in their lives. Within the security branch of this ministry, the Nationaal Coordinator Terrorismebestrijding en Veiligheid[78] (NCTV) is responsible for policies concerning Counterterrorism, National Security, Cyber Security and Crisis Management[79]. It has the overall coordination role for the national approach to Hybrid Threats.

- Buitenlandse Zaken[80] (BuZa). The Ministry of Foreign Affairs is working for Dutch people and Dutch interests and values, all over the world. Within this ministry the Directorate Security Policies is handling themes concerning international peace and stability and is responsible for the Dutch contribution in international organisations like EU, NATO and UN[81].

- Defensie[82] (MinDef). MinDef provides peace and security, both nationally and internationally by: Defending Dutch and alliance territory; participating in peace and stability operations worldwide; and participating in national security under civil authority[83]. MinDef is the political instrument for applying armed force, in case necessary.

This selection has been done based on the snowball method. When searching for actors involved in Hybrid Warfare, a Leiden University Staff member advised to contact MinDef. The point of contact at MinDef arranged an introduction to BuZa and JenV. And although Hybrid Threats are relevant to the whole society, suggesting that many more ministries and agencies should be involved, it became clear that only these 3 ministries already put Hybrid Threats on the agenda and had dedicated personal assigned to the topic.

The documents examination will consist of 3 elements. For documents that are released regularly, like the national budget, a comparison will be made between 2015 (before the EU

[77] Ministry of Justice and Security.
[78] National Coordinator Counter Terrorism and Security.
[79] Corporate folder NCTV, p. 6. https://english.nctv.nl/binaries/nctv-brochure-2014-en-lores-spreads_tcm32-84088.pdf
[80] Ministry of Foreign Affairs.
[81] https://www.rijksoverheid.nl/ministeries/ministerie-van-buitenlandse-zaken/organisatie/organogram/themadirecties
[82] Ministry of Defence.
[83] Rijksbegroting 2018 Defensie, Tweede Kamer, vergaderjaar 2017–2018, 34 775 X, nr. 2, p. 14.

policy was released) and 2018 (2 years after the EU policy was released, for this period the EU has reported significant progress). For documents that are not released on regular basis, the current version will be checked to see whether they contain one or more of the given indicators. Finally the websites of the three ministries will be scrutinised to determine if Hybrid Threats are already mentioned.

The regularly released documents that will be examined are the *Rijksbegroting*[84] for the 3 ministries and *Internationale Veiligheidsstrategie*[85]. The non-regular document is *Tweede kamer brief Ongewenste Buitenlandse Inmenging*[86] which is, according to respondent 1, *the* document reflecting the current vision on Hybrid.

The chosen documents are policy documents and should provide clear insight in the development of Dutch polices for countering Hybrid Threats. No dedicated section or dossier on Hybrid Threat could be found in governmental sources, so the actual list of related documents, reports, notes and food-for-thought papers could be longer. In order to make sure that all relevant indicators are addressed and the relevant sources are included, interviews with representatives of all 3 ministries have been conducted. Part of their contribution was to point out documents that should (also) be investigated. The other part was that they provided factual information on the Dutch approach and helped to outline the national and international context in which the Hybrid Threat discussion is conducted.

All interviewees work in the security branches of their ministries, and are considered to be the primary point of contact for Hybrid Threats. For security reasons one of the respondents does not want his/her name and job title to be published. Therefor no names will be used[87]. The respondents will be referred to as: respondent 1 for JenV, respondent 2 for BuZa and respondent 3 for MinDef.

4.6 ANALYSES

The analysis will be performed in three steps. First a straight forward search whether the concept of Hybrid Threat is mentioned, and if so how often. An increase of the use of the concept might indicate a growing attention to it. Then the context in which the concept is used will be examined. Is the concept used as part of a policy or action, or is it used in a more

[84] National Budget.

[85] National Budget and International Security Strategy.

[86] Letter to Parliament Unwanted Foreign Interference.

[87] Names and job titles are known by the thesis supervisor.

general context, and did the respondents add any useful information to what has been written? Finally a search will be performed for policies and actions in the security environment that are affiliated to Hybrid, but are named differently. The concept Hybrid is complex by nature, and is a new kid on the block. It is not unthinkable that existing policies are already developing is such a way that they line-up with the EU policy on Hybrid, without the policy-makers realising it.

4.7 BOUNDARIES

Boundary in time: The Joint Framework was released in 2016. So the starting point in this study is a year prior to that event. Policies up to that point cannot have been influenced by the Framework and will serve as the base-line. The ending point is mid-June 2018, when the second progress report was released. If any, chances can be observed in that timeframe.

Boundaries in content: Hybrid Threats is about security, vulnerabilities and actions to prevent an opponent to exploit ones vulnerabilities. It is easy to understand that a lot of the information is classified and cannot be exposed to the public, not even to highly educated scholars. This study will not use any classified information, only open sources have been used. I did use my opportunity to interview representatives from the Military Cyber Command and the Military Intelligence and Security Service[88]. But these conversations were either too detailed and therefor classified, and when avoiding sensitive information, they became superficial and reflected open source information as can be found in the body of knowledge. The interviews did help the author to gain more insight in the concept, but the content of those interviews will not be used. More or less the same applies to the respondents that participated. They also deal with security and one should keep in mind that they are not free to discuss everything in detail. Is that a shortcoming? No! When investigating tactics, techniques and procedures, one cannot without subject matter experts and then it cannot be avoided that classified information is required. When investigating whether EU initiatives are being accepted and implemented, there is no need for to go deeper than the freely available information.

[88] Author does posses a national security clearance.

4.8 VALIDITY

Internal validity[89]: in qualitative studies this is also called *Credibility* and sees on producing results that are credible rather than provable. Credibility is judged by the approval of those participated in the research. The findings of the analyses has been presented to the respondents who confirmed that their inputs were used in a proper way.

Furthermore internal validity is about measuring what is actually being researched. The clear construction of the indicators, the explanation of the data collection and analysis and the given boundaries all lead to the answer to the R.Q..

External validity: this refers to the extent to which the results can be generalised or transferred to other context settings. Generalisation is hardly possible in single case studies, since these are aimed at gaining deep insights in one particular situation. But generalisation is not the aim of this thesis. Despite some argue differently, single case studies can contribute to scientific development[90]. It is difficult to establish transferability, primarily because of the approach in qualitative research. The process as described in this chapter should provide enough guidance others to follow and replicate.

Reliability: this is concerned with whether the same results would be obtained if the same research would be done again. The process as described in this chapter should provide enough guidance to others to follow and replicate the study. Still it will be unlikely that exactly the same findings will be found since qualitative studies leave space for each researcher to work from their own frame of reference, thus introducing differences in interpretation. The same goes for the use of interviews. Respondents will not always answer exactly the same on the same question, the context of the interview might be slightly different, time has passed and facts have sunk deeper in the memory of the respondents, or new views have arisen which can divert a new interview from the path that was followed in this research.

[89] Definitions of validity and reliability according to Trochim and Donnely, quoted in: Ranjit Kumar, research methodology a step-by-step guide for beginners 3rd edition, SAGE Publications Ltd, 2011, p. 172

[90] Bent Flyvbjerg, Five Misunderstandings About Case-Study Research, Qualitative Inquiry Volume 12 Number 2 April 2006, p. 221.

5 THE EUROPEAN UNION AND HYBRID

5.1 THE EU TAKES AN INTEREST IN HYBRID THREATS

In the US the concept of Hybrid War was already addressed in 2002, in Europe it took until 2010 before it made its way the security agenda. One of the first major policy documents that addressed this concept was NATO's Strategic Concept for 2010, which also included the NATO Capstone Concept (as discussed in chapter 2.5). One of the chapters in the Strategic Concept deals with partnerships. One of the essential partners for NATO is the EU since these organisations share a majority of members, and all member states share common values. It is noted that NATO and the EU should complement and mutually reinforce their activities in supporting international peace and security. Another important partnership is that with Russia. Key issue in the NATO-Russia relationship is the respect of democratic principles and the sovereignty, independence and territorial integrity of all states in the Euro-Atlantic area. Notwithstanding differences on particular issues, NATO remained convinced that the security of NATO and Russia is intertwined and that a strong and constructive partnership based on mutual confidence, transparency and predictability can best serve security[91].

Like NATO, the EU is dealing with security questions, both inside and outside the Union. After the Lisbon Treaty, which came in effect on 1 December 2009, the post of High Representative of the Union for Foreign Affairs and Security, who is also Vice-President of the Commission, was created, and the European External Action Service (EEAS) was established. By this, the EU increased its potential – by drawing on the full range of its instruments and resources – to make its external action more consistent, more effective and more strategic. Working on international peace and security, the EU launched "the comprehensive approach to external conflicts and crises" in 2013. This document explains that, in order to apply the EU external policy, all stages of a conflict should be taken into account: "early warning and preparedness, conflict prevention, crisis response and management to early recovery, stabilisation and peace-building in order to help countries getting back on track towards sustainable long-term development."

Being the world's largest trading block, it is in the EU's interest to have global peace and stability. The Union has a wide variety of policies, tools and instruments that can be applied

[91] Active Engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, p. 28-29. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

in order to counter security challenges – spanning the diplomatic, security, defence, financial, trade, development cooperation and humanitarian aid fields. It is noted that global challenges getting more and more in number and the complexity of these challenges is increasing (effects of climate change and degradation of natural resources, population pressures and migratory flows, illicit trafficking, energy security, natural disasters, cyber security, maritime security, regional conflicts, radicalisation and terrorism, et cetera). At the same time economic and financial resources remain under pressure. This combination of factors calls for an (integrated) comprehensive approach, making optimal use of all relevant instruments[92].

This policy document was fully committed on keeping or bringing peace and stability to instable countries outside the Union. The term Hybrid Warfare was never mentioned. Not in the context that violent groups or states were waging Hybrid War to destabilise countries outside the Union, thus interfering with EU's international interests. And definitely not in the context that it could be conducted against the Union and its member states.

First in 2015, after Russia's actions in Ukraine and the ISIS/Da'esh campaign in Iraq, the concept of Hybrid Warfare got full attention from the EU. In February 2015, EU Defence Ministers called for more unity and concrete action at EU level. In May 2015, the EEAS drafted and released a 'food-for-thought paper Countering hybrid threats', which stated that the EU needs to be able to recognise hybrid threats and the effects, and that these threats should be countered by building more resilience[93]. In reaction to this 'food-for-thought paper', the EU Foreign Affairs Council invited the European Commission and the High Representative to develop a joint framework on Hybrid Threats. This framework should not so much describe the concept, but should streamline existing policies on security and to come up with concrete proposals on how to deal with Hybrid Threats.

Noteworthy in this process is that, even though a lot of EU member states are also NATO member, the EU did not adopt the aggressive sounding term *Warfare* as NATO uses, but choose to refer to the concept as Hybrid Threats. This might not be that surprising, since for a long time many member states did not want to be involved in contemporary international turmoil. They preferred to see Europe as a provider of soft power, dedicated to intervening

[92] JOIN (2013) 30 final, The EU's comprehensive approach to external conflict and crises, Brussels, Dec.2013, p. 2-3.
[93] Patryk Pawlak, Understanding hybrid threats, European Parliamentary Research Service, June 2015, p. 1.

with political and economic means, rather than a provider of hard power that tries to adjust unfavourable situations through the use of military force[94].

5.2 JOINT FRAMEWORK ON COUNTERING HYBRID THREATS: AN OVERVIEW

The "*joint framework on countering Hybrid Threats*[95]" was released in April 2016. The document starts with defining the concept and the context. It is noted that there is a multitude of definitions of hybrid threats, and considers that to be good thing because such a diversity provides the necessary flexibility to respond to their evolving nature. In general the concept of Hybrid Threats "*aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare"*. Key elements are exploiting the vulnerabilities of the target and generating ambiguity which will hamper decision-making. Disinformation campaigns, launched by adversaries, using social media to control the political narrative or to radicalise, recruit and direct proxy actors are described as vehicles for hybrid threats. Notice that, according to the framework, the information domain is no part of the threat (or as you wish: no instrument of power), it is only seen as an enabler.

This is remarkable since disinformation can seriously undermine democracies and their values. There are many commercial companies in Russia that are paid by the government to target the West by spreading fake news[96]. The Russian government is also behind news channels like RT and Sputnik that are using Western "experts" to influence the Western audience. This, in combination with the use of trolls, that systematically deny facts, create confusion and have a counter-narrative for every Western narrative, has created distrust against regular media on a global scale[97].

Vulnerabilities vary from country to country. Therefor the primary responsibility for countering Hybrid Treats rests with the individual member states. However, many of threats faced by member are common, or target networks or infrastructures that are shared by

[94] Daniel Fiott et al, The common security and defence policy: national perspectives, Egmont Paper 79, May 2015, p. 9.

[95] JOIN(2016) 18 final, Joint Framework on countering hybrid threats; a European Union response, Brussels, Apr.2016, pp. 2-18.

[96] Prof. dr. Rob de Wijk, Hybride dreigingen, in Magazine Nationale veiligheid en crisisbeheersing, Thema Hybride dreigingen, 14e jaargang 2016 nr. 5/6, p. 14.

[97] Laura Starink, Hubert Smeets, Ruslands machtspolitiek: voor staat, taal en kerk, in Magazine Nationale veiligheid en crisisbeheersing, Thema Hybride dreigingen, 14e jaargang 2016 nr. 5/6, p. 28-29.

multiple member states. Such threats can be countered more effectively with a coordinated response at EU level by using EU policies and instruments, by demonstrating European solidarity, and by providing mutual assistance. The joint framework is not so much about developing new tools, rather it is about creating synergies between existing strategies and sectoral policies that contribute to achieving security, and about promoting cooperation between all actors. As for the use of existing policies, the framework states that "in particular, the European Agenda on Security, the upcoming European Union Global Strategy for foreign and security policy and European Defence Action Plan, the EU Cybersecurity Strategy, the Energy Security Strategy, the European Union Maritime Security Strategy are tools that may also contribute to countering hybrid threats".

The framework focuses on 3 elements: Improving awareness; Building resilience; Preventing and responding to crisis and recovering. It contains a total of 22 actions for both the European Commission and the individual member states.

Improving awareness should start with assessing vulnerabilities and creating threat indicators and continuously monitoring them. In order to assist the member states and to improve information sharing, the framework advices to establish a European Centre of Excellence (CoE) for designing strategies to counter hybrid threats, and to set up an EU hybrid fusion cell that will analyse and share information relating to indicators and warnings concerning hybrid threats. To raise public awareness about hybrid threats and to mitigate the effects of disinformation campaigns, a strategic communication strategy should be developed. All initiatives should seek cooperation with other stakeholders such as NATO, regional organisations and the private sector.

Building resilience (the capacity to withstand stress and recover, strengthened from challenges) by; protecting critical infrastructure (e.g. energy, transportation, space); developing defence capabilities; protecting public health and food security; improving cybersecurity; targeting hybrid threat financing; fighting radicalisation and violent extremism; and by increasing cooperation with third countries.

Preventing, responding to crisis and recovering. The EU will use existing mechanisms such as the European Emergency Response Coordination Centre or EU Integrated Political Crisis Response (IPCR), and Treaty-based instruments like the Solidarity Clause or Mutual Assistance Clause. The Common Security and Defence Policy should be leading in setting up civilian and military training, advisory missions to improve the capacities of states under

threat, contingency planning and strengthening early warning capabilities, support for border control management, and specialised support in areas such as chemical, biological, radiological or nuclear (CBRN) risk mitigation or non-combatant evacuation.
Increasing cooperation with NATO. Not only the EU is confronted with Hybrid Threats, also the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE) and NATO face similar threats. Especially cooperation with NATO, to ensure complementarity of measures undertaken on situational awareness, strategic communication, cybersecurity and crisis response, is promoted in this framework.

5.3 Implementing the Joint Framework, what has been achieved in year 1?

As requested by the Council[98], the High Representative presented a progress report on countering Hybrid Threats in July 2017[99], which was accompanied by a press release[100].

Improving awareness; a group called "Friends of the Presidency" has been established that will build a generic survey to will help the member states to identify vulnerabilities and indicators to recognise threats.
Finland has established the EU Centre of Excellence for countering Hybrid threats. Finland, France, Germany, Latvia, Lithuania, Poland, Sweden, United Kingdom, Estonia and Spain were the first member states to join this CoE, and were joined by non-member states Norway and US[101]. The Centre's mission is to encourage strategic dialogue and do research in order to improve resilience and ability to respond. It will also play an important role in future hybrid exercises.
In order to receive and analyse information, a Hybrid Fusion Cell has been created that has started the release of a periodical bulletin. The Cell is already cooperating with the CoE and NATO, and is investigating ways to further improve a joint approach.
On the subject of awareness and misinformation, the High Representative has installed East Stratcom Task Force which forecasts and responds to disinformation cases and campaigns. Also a new and user friendly website will be launched (#EUvsdisinformation) that will help

[98] Council conclusions on countering hybrid threats, Press Release 196/16, 19 April 2016.
[99] JOIN(2017) 30 final, joint report to the European parliament and the Council
on the implementation of the Joint Framework on countering hybrid threats - a European Union response, Brussels, 19.7.2017.
[100] Security and defence: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead, European Commission - Press release, Brussels, 19 July 2017.
[101] on May 28 2018, the website shows 2 additional member states as well as NATO and EU, https://www.hybridcoe.fi/about-us/

citizens to better recognise disinformation. It is noted that the amount of information is so enormous that it will be impossible to unmask all misleading information.

Building resilience; Many of the action items are still in the research phase in which the key issues are investigated and plans are drafted. The main effort has been on streamlining awareness on hybrid in many sectors, including energy, transportation, customs, space, health and finance. Working in close relation with the European Aviation Safety Agency, a Computer Emergency Response Team on Aviation and a Task Force on Cyber-security have been established. As for defence, a number of exercises have been conducted. The results of these exercises will be incorporated into the Capability Development Plan. In the cyber area, the 2013 EU Cybersecurity Strategy is reviewed, in order to come to a more integrated and coordinate response to cyber threats.

Preventing, responding to crisis and recovering; To establish a common operational protocol and to improve strategic decision-making capacity, the Commission services and the EEAS issued the EU operational protocol for countering hybrid threats (EU Playbook) which was adopted in July 2016. This playbook outlines the requirements for coordination, intelligence fusion and analysis, informing policy-makers, exercises and training, and cooperation with partner organisations. To test the usefulness of the playbook, a joint EU – NATO exercise is planned.

Increasing cooperation with NATO; On the basis of a joint declaration, signed on 8 July 2016, the EU and NATO developed a common set of 42 proposals for implementation. In June 2017, the High Representative/Vice President and the Secretary General of NATO published a report on the overall progress made on the 42 actions. Countering hybrid threats is one of the seven areas of cooperation identified. The report presents substantial results, created by joint efforts undertaken over the past year. In 2017, NATO and the EU staffs will exercise together their response to a hybrid scenario. This exercise is expected to test the implementation of a part of the common proposals. The EU will carry out its own parallel and coordinated exercise and is preparing to take a leading role in 2018.

5.4 Implementing the Joint Framework, what has been achieved in year 2?

The second annual report on the implementation of the Joint Framework on countering Hybrid Threats was released on 13 June 2018[102], also accompanied by a press release[103]. Again it claims that "Considerable progress has been made in all four priority areas of action". The first thing that draws attention is that there are no longer 3 focus areas, the cooperation with NATO has also become a priority area. In an additional report[104], special attention is given to CBRN threats. The Salisbury nerve agent attack drew attention to the need for resilience against those threats. Because of the difficulties in detecting, attributing and recovering from those threats, as well as the possibility for large scale damage, the CBRN threats fall in a category of their own. A separate Action Plan on this topic was released in 2017[105].

Improving awareness; in this focus area, the most concrete actions were taken in the first year, like the establishment of a CoE, a Fusion Cell and a StratCom Task Force. After this second year some concrete results can be reported.

On initiative of The Friends of Presidency Group, member states have started to conduct surveys to assess their vulnerabilities. The Fusion Cell has produced over 100 reports that were shared amongst the member states. Furthermore it has set up a network of National Points of Contact, and has set up relations with the CoE and NATO.

The StratCom Task Force is monitoring disinformation (identifying over 4000 cases of disinformation), raising awareness, training Partnership countries and is developing positive narratives.

The CoE has supported member states through research, training, education and exercises. It also released several analysis and hosted a number of high level meetings to share information and to improve common knowledge.

Building resilience; This area is policy-heavy and it is very difficult to measure the results. The overall tendency is that existing policies and legislation are under revision and that some new policies have been proposed. These actions are not necessarily specific to Hybrid

[102] JOIN(2018) 14 final, on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018, Brussels, 13.6.2018.

[103] A Europe that protects: EU works to build resilience and better counter hybrid threats, Brussels, 13 June 2018, http://europa.eu/rapid/press-release_IP-18-4123_en.htm

[104] JOIN(2018) 16 final, Increasing resilience and bolstering capabilities to address hybrid threats, Brussels, 13.6.2018, p. 1.

[105] COM(2017) 610 final, Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, Brussels, 18.10.2017.

Threats, but when they are reviewed in conjunction, they can enhance resilience and make the EU more capable in countering Hybrid Threats.

Preventing, responding to crisis and recovering; The main achievement in this area is the establishment of the EU Operational Protocol for crisis response. Although the main effort is in preventing and mitigating Hybrid Threats, once they occur, they must be dealt with in a swift and consistent manner. Tested during the combined EU/NATO exercise EUPACE17, the protocol proved its value as a tool to connect separate services, and "provided the touch points for interaction between the various levels of response: political strategic, operational and technical, as well as between the three main EU response mechanisms of Crisis Response (for external crises), ARGUS (the Commission internal IT based platform for information sharing) and the Council's Integrated Political Crisis Response platform".

Increasing cooperation with NATO; Countering Hybrid Threats is a key area of EU-NATO cooperation. During PACE17 NATO and EU exercised jointly and gained viable information on the capability to act together in case of an Hybrid Attack. The joint approach will be continued with more exercises to come, and the participation of NATO in the CoE .

5.5 From Union towards member state

In this chapter we have seen that the EU first put the concept of Hybrid Warfare on the security agenda in 2015, where in the US this concept was already adopted in the early years of the 21st century. That does not mean that the EU is ignorant on this subject. The EU was already using the Comprehensive Approach. As we have seen before, some claim that "Hybrid War is the Comprehensive Approach gone to the dark side". If you understand how the Comprehensive Approach can be used with good intentions, it is not so difficult to understand how the same tools can be used with bad intentions, and that call it Hybrid Threats. Furthermore the EU already had several separate policies on security. Picking up the concept of Hybrid Threat was not about inventing new policies, rather it was about creating synergies between existing strategies and sectoral policies that contribute to achieving security, and about promoting cooperation between all actors. The Joint Framework intents to do so. Reviewing, adjusting and streamlining is a time consuming process which has started after adoption of the framework. After 2 years the Commission and the High Representative claim significant progress on all aspects, but only a few concrete, visible results can be presented. The EU Hybrid Fusion Cell was established, Finland has opened the European Centre of Excellence for Countering Hybrid Threats, Communication Task Forces for neighbourhoods have been established, a Computer Emergency Response Team on Aviation as well as a Task Force on Cyber-security became operational.

These are the initiatives on a Union level. In the next chapter we will see what has been achieved on member state level. For that, it will be investigated in what way the Joint Framework has guided member state the Netherlands in improving her capabilities to counter Hybrid Threats.

6 FINDINGS AND ANALYSIS.

6.1 INTRODUCTION

In this chapter the findings and the analysis of the findings will be presented. For each indicator the used data will be listed, the relevant finding will be noted and a reflection will be given. Each paragraph will end with a summary of the findings.

6.2 INDICATOR: THE CONCEPT OF HYBRID THREATS IS INCORPORATED IN POLICY DOCUMENTS.

The first thing that draws attention is the definition. The EU uses the term Hybrid Threats, The Netherlands has chosen to name it Hybrid Conflict[106]. From a linguistic point of view, this puts it somewhere in between "a suggestion that something unpleasant or violent will happen" (i.e. Threat, as used by EU) and "the activity of fighting a war, often including the weapons and methods that are used" (i.e., Warfare, as used for example by NATO). The word conflict seems to be a smart choice since it can mean two things: "an active disagreement between people with opposing opinions or principles" or "fighting between two or more groups of people or countries[107]". Going with the first definition it indicates that non-friendly actions are not just a possibility but are already in progress, and puts a certain amount of urgency on activities to counter-act or defend form those non-friendly activities. In case the active disagreement escalates, the second meaning of conflict makes it possible to keep using the term Hybrid Conflict, without the need to upgrade it to the term warfare (for which a declaration of war is needed as we have seen in chapter 3.2).
Furthermore the content of the Dutch definition differs slightly from the EUs definition.

NL[108]: "*conflict between states, largely under the legal level of openly armed conflict, with integrated use of resources and actors, with the aim of achieving certain strategic objectives*".

EU: *"the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare"*.

[106] Definition was provided by a staff member of JenV via e-mail dated 30-08-2017. See also Nationaal Veiligheidsprofiel 2016, p. 14.
[107] All definitions taken from the Cambridge Advanced Learner's Dictionary & Thesaurus. https://dictionary.cambridge.org/dictionary/english
[108] Authors translation of the definition provide by JenV in Dutch.

The first difference is a result from the choice in naming as explained before. The EU uses "threats", so the definition is about "activities that can be used", the Netherlands sees it as "conflict" which indicates that something is already going on.

More substantial is the difference between the actors. The EU assumes that both state and non-state actors are able to coordinate means and activities in such a way that they constitute a threat. The Netherlands has explicitly excluded the non-state actors. It is their opinion that non-state actors do neither have strategical objectives, nor the capacity to coordinate and direct instruments of (state) power in such a way that they can initiate and maintain a Hybrid Conflict. The Dutch consider non-states actors to be one of the means (a proxy) that can be used within a Hybrid Conflict[109].

Respondent 1 did acknowledge the differences in definition but stated that these are minor differences that in no strong way hampers coordination and cooperation with the EU or other member states. Bearing in mind that there are many definitions of the concept used, he considers it not useful to invest time and effort to come to a full alignment of definitions.

Remarkable in this case is that in certain national fora the topic is referred to as "Unwanted Foreign Influence[110]", defined as "deliberate, often systematic and in many cases secret activities of state actors (or actors that can be related to state actors) in the Netherlands or aimed at Dutch interests." This is considered to be highly undesirable since "state actors can come to the foundation of the Dutch democratic legal order and open society: the integrity of political and administrative decision-making, independent justice, free and fair elections and fundamental freedoms such as press freedom and freedom of expression. In addition, unwanted foreign interference can lead to tensions within and between population groups in the Netherlands[111]". The remainder of the letter focusses on individual undermining actions by foreign actors. It does specify that an integrated use of a variety of means by a state actor

[109] This paragraph is a reproduction of the fore mentioned mail by JenV.

[110] National Budget Justice and Security, Tweede Kamer, vergaderjaar 2017–2018, 34 775 VI, nr. 2, footnote 8, p. 18. See also: Brief ongewenste buitenlandse inmenging, Nationaal Coördinator Terrorismebestrijding en Veiligheid, kenmerk 2223363, 16 maart 2018. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022, Wereldwijd voor een veilig Nederland, 14-05-2018, p. 34. https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs

[111] Brief ongewenste buitenlandse inmenging, Nationaal Coördinator Terrorismebestrijding en Veiligheid, kenmerk 2223363, 16 maart 2018. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022, Wereldwijd voor een veilig Nederland, 14-05-2018, p. 34.

to achieve strategical goals is called Hybrid Threat or Conflict. Hybrid Conflict seems to be the higher level, the more integrated and the more deliberate way of influencing society.

Next the policy agendas in the National Budget[112] will be explored. The initial search has been to see whether Hybrid is mentioned in those documents. For all 3 departments goes: in 2015 there is no reference to the concept of Hybrid at all, in 2018 the word Hybrid is used once.

In the policy agenda, JenV describes a number of areas in which cooperation with private companies and national and international partners is needed to improve security. Among these areas are organised crime, terrorism, cybercrime and migration. Within these areas an integrated approach is required, there is only one indication that there is an overarching effort to integrate these areas. The only thing mentioned is that national and international coordinated actions are prepared and taken in order to counter Hybrid Threats[113].

In the policy agenda BuZa uses the term to explain the still increasing complexity of the security environment (and includes non-state actors in the threat[114], so they deviate from the Dutch definition). In the security paragraph the threats by terrorism, cyberattacks and instability on the South and East flanks are mentioned. The need for a 3-D approach (Development, Defence and Diplomacy[115]) to deal with these threats is emphasised, as well as the cooperation with NATO and EU. It also mentions that Unwanted Foreign Influence is increasing[116]. But this is just a standalone sentence, no further explanation is given and no indications are given that there is an overarching effort to counter this.

MinDef uses the term only to justify the establishment of a Special Operations Command[117]. The document is mainly about getting the military back on the level in which it can be effectively used as an instrument of power.

[112] The 6 documents used are:
National Budget Security and Justice, Tweede Kamer, vergaderjaar 2014–2015, 34 000 VI, nr. 2
National Budget Justice and Security, Tweede Kamer, vergaderjaar 2017–2018, 34 775 VI, nr.2
National Budget Foreign Affairs, Tweede Kamer, vergaderjaar 2014–2015, 34 000 V, nr. 1
National Budget Foreign Affairs, Tweede Kamer, vergaderjaar 2017–2018, 34 775 V, nr. 1
National Budget Defence, Tweede Kamer, vergaderjaar 2014–2015, 34 000 X, nr. 2
National Budget Defence, Tweede Kamer, vergaderjaar 2017–2018, 34 775 X, nr. 1

[113] National Budget Justice and Security 2018, Page 18.

[114] National Budget Foreign Affairs 2018, Page 7.

[115] https://www.rijksoverheid.nl/onderwerpen/internationale-vrede-en-veiligheid

[116] National Budget Foreign Affairs 2018, Page 9.

[117] National Budget Defence 2018, Page 8.

The next documents that where compared for this indicator are the International Security Strategy (IVS[118]) 2013 and its successor[119] the Integrated Foreign and Security Strategy (GBVS[120]) 2018. Since there was no IVS released in 2015, the 2013 version was most recent one before that year and is therefore used.

The term Hybrid is not used in the IVS 2013. In the GBVS the word Hybrid is mentioned 12 times, all times to emphasis the complexity of the international security environment and the need to come to (national and international) integrated policies. The GBVS, which is written in line with the European. Union Global Strategy (EUGS), is connected to several policy areas, like cyber, police and counter terrorism, but does not see Hybrid as a separate area; there is no "Hybrid strategy". Neither is Hybrid mentioned as the interconnection between the separate policy fields.

What is mentioned, is the fact that "there will be one common Dutch approach against Unwanted Foreign Influence[121]". As we have seen before, the terms Hybrid Threats and Unwanted Foreign Influence are closely related, but not the same. This one common approach appears to be coming close to a policy on Hybrid Threats.

The Letter on "Unwanted Foreign Influence" the Dutch government recognises that foreign powers abuse the openness of the Dutch society to influence it. Several measures are taken to create resilience, focussing on defensible citizens, independent media, diversity in the political arena and countering disinformation. Although emphasis is put on a coordinated development and use of those measures, the letter does not show any form of integration.

When addressing Hybrid Threats, it is noted that EU cooperation is considered to be essential in countering those threats. This suggests that the Netherlands feels threatened by individual threats (without a strategic driver), the EU is threatened by a combination of threats (which are strategically driven), thus becoming Hybrid Threats. It is significant to note that the Dutch government explicitly refers to the EU Framework as *the* instrument that can help.

[118] Internationale Veiligheidsstrategie, Veilige Wereld, Veilig Nederland, 21-06-2013, https://www.rijksoverheid.nl/documenten/rapporten/2013/06/21/veilige-wereld-veilig-nederland-internationale-veiligheidsstrategie

[119] This relation is directly stated in Kamerbrief Geïntegreerde Buitenland- en Veiligheids Strategie, p. 1. https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/20/kamerbrief-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs

[120] Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022, Wereldwijd voor een veilig Nederland, 14-05-2018, https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs

[121] GBVS, P.34.

Furthermore is stated that the Netherlands contributes to the CoE on Countering Hybrid Threats and participates in EU/NATO exercises in which attention is given to Hybrid Threats[122]. It is the authors opinion that this would be *the* place to mention any Dutch policies and/or activities in the field of Hybrid Threats. But that statement is missing, suggesting that such a policy does not exist.

Another check has been performed on existing policies, like cyber, counterterrorism and the national security strategy. The open source policies can be found on the site of the NCTV. All these policies are applicable for the period 2016- 2020, and were released in 2016. None of these has been updated since. Therefore the EU policy can not be incorporated in these individual policies. (a quick scan shows that indeed it is not)

The last check to see if there are existing policies on Hybrid is performed on the websites of the ministries. These sites of course provide general information to citizens and do not provide hard evidence for the presence or absence of policies, but in combination with the above findings it does add to the complete picture.

The site JenV.nl[123] gives an overview of the portfolio distribution[124] within the ministry. It shows several individual policies like Counterterrorism, National Security, Cybersecurity, human trafficking and migration. Neither of the two ministers, nor the Secretary of State has a policy on Hybrid Threats assigned. Going one step deeper in the organisation leads us to the National Coordinator for Security and Counterterrorism (furthermore referred to as NCTV: Nationaal Coordinator Terrorismebestrijding en Veiligheid). The NCTV deals with several security related dossiers like cyber, terrorism, extremism and CBRN[125]. For these dossiers separate information pages are available, none of them mentions the term Hybrid, neither does a separate dossier on Hybrid exist.

Buza.nl[126] does have a section dealing with peace and security and refers to the 3-D Approach as the way to bring peace and prosperity, there is no mentioning of Hybrid Threats. This 3-D Approach is also known as the Comprehensive Approach (CA). We have seen in chapter 3.1 that Hybrid Warfare is seen as "Comprehensive Approach gone to the dark side". This site

[122] Brief ongewenste buitenlandse inmenging, Nationaal Coördinator Terrorismebestrijding en Veilighei d, kenmerk 2223363, 16 maart 2018, p. 3.
[123] https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid
[124] https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/organisatie/portefeuilleverdeling
[125] https://www.nctv.nl/onderwerpen_a_z/
[126] https://www.rijksoverheid.nl/ministeries/ministerie-van-buitenlandse-zaken

therefor pays attention to how the Netherlands tries to help foreign states, but it does not inform the public that other states try to influence the Netherlands through hybrid tactics. Mindef.nl[127] does not give any hit on the term Hybrid. On the tab *subjects*, it provides general information over the organisation, including on several operational missions, but no specific dossier on Hybrid can be found.

For the indicator: the concept of Hybrid Threats is incorporated in policy documents; no evidence can be found in open sources that a dedicated policy on Hybrid Threats exists, neither that existing policies have been updated in order to align them with the EU policy. The existing Dutch definition has been compared to the EU definition and was already sufficiently aligned. Although the term is used in letters and documents, it is mostly used to describe the complexity of the security arena. The only indication of an integrated approach to Hybrid Threats is linked to the EU Joint Framework. It appears that the common policy on Unwanted Foreign Influence comes close to a national policy on Hybrid Threats. But not mentioning the existence of a policy when reporting to parliament on "Unwanted Foreign Influence", suggests that there is no separate policy.

6.3 INDICATOR: BUDGETS ARE ASSIGNED TO COUNTER HYBRID THREATS

For this indicator the National Budgets will be explored. Since the term Hybrid Threats was never mentioned in 2015, there will be no comparison between the two years. Only 2018 will be examined.

The first that is examined is the JenV National Budget. There is no budget directly assigned for dealing with Hybrid Threats. That of course is logical since the term is only used once, in a descriptive way. In the policy area Counterterrorism and National Security some links can be found. Budget is assigned to identify and assess threats to national security[128]. The aim of Counterterrorism and National security is contributing to a safe and stable Netherlands by preventing and limiting social disruption by recognizing threats, increasing the resilience of citizens, the business community and government bodies and strengthening the protection of vital assets[129]. This text aligns to a great extent with the Joint Framework (chapter 6), but is in this National Budget not linked to Hybrid. So budgets assigned to Counterterrorism and

[127] http://www.defensie.nl/

[128] National Budget Justice and Security 2018, P.30, point 36.

[129] National Budget Justice and Security 2018, P. 71.

National Security cannot be linked to countering Hybrid Threats. Further no possible links could be found.

The BuZa National Budget gives an overview of the budgets that are assigned to security[130]. In the explanation in the chapter on security and stability it becomes clear that the budgets are for individual policy areas like; to counter terrorism, to fight organised crime, to contribute to stability operations and to contribute to international cooperation in order to improve common security. The only indication of any new form of integration of policies is that the Netherlands will support the efforts of the Global Counter Terrorism Forum to investigate the potential link between organised crime and terrorism. This is described as deepening of an existing policy, not as a step towards an integrated approach on Hybrid Threats. Any direct financial link to Hybrid cannot be found.

In the MinDef National Budget, there is no real link to Hybrid, and no indicators could be found that funds are assigned to it.

A further indication is found in the letter on "Unwanted Foreign Influence", in which a high level description is given of the measures taken to counter different forms of influence. The only reference to financial means is in the part on disinformation. It calls for intensive European cooperation, but states that all efforts have to be done within the existing budget[131].

A circumstantial indication can be found in another letter to parliament[132]. The Netherlands did have a Budget International Security, which was shared by Defence, BuZA and Foreign Trade and Development to finance coordinated activities. Evaluation showed that this shared fund did not stimulate the coordinated approach to security, therefore it was lifted and the money was divided over the departments. Where Hybrid Threats call for an integrated and coordinated approach, lifting a shared fund for security indicates an movement in opposite direction.

The only evidence that a budget is assigned to counter Hybrid Threats comes from respondent 3. He indicated that, as of 2018, Defence has assigned an annual budget to accommodate a dedicated Hybrid Warfare Cell.

[130] National Budget Foreign Affairs 2018, P. 23. Sub article 2.1 – 2.5.

[131] Brief ongewenste buitenlandse inmenging, Nationaal Coördinator Terrorismebestrijding en Veiligheid, kenmerk 2223363, 16 maart 2018, P. 5.

[132] Beleidsdoorlichting Defensie, brief van de ministers van defensie, van buitenlandse zaken, voor buitenlandse handel en ontwikkelingssamenwerking en van justitie en veiligheid, Den Haag, 28 maart 2018, p.2. https://zoek.officielebekendmakingen.nl/kst-31516-23.html

For the indicator: Budgets are assigned to counter Hybrid Threats; only one piece of evidence could be found. Jenv and BuZa do invest in security, but all budgets are assigned to individual policy areas, any new efforts are to be done within existing budgets. Only Defence has assigned a dedicated budget to deal with Hybrid Threats.

6.4 Indicator: National or international organisational elements dealing with Hybrid Threats are (being) established.

In all 3 National Budgets, no evidence can be found that organisational elements are established. Since all 3 hardly mention the concept of Hybrid Threats, no policies can be found and no budgets are assigned, this finding was expected.

In the GBVS is written that for an effective approach to security a coherent policy is required in which strategic goals and a wide variety of means are interconnected. The GBVS is therefore linked to existing policy areas such as the strengthening and modernization of the armed forces, the foreign trade and development cooperation policy, the integrated migration agenda, the commitment to economic security, the intelligence and security services, the Dutch Cyber Security Agenda, the Digitization Agenda, the International Police Strategy and the National Counterterrorism Strategy. It than continues "No separate consultation or decision-making structures are set up for the implementation of the GBVS. The strategic deployment within the three pillars (Prevent, Defend and Strengthen) is reflected in (inter) departmental policy and operational plans[133]."

Respondent 3 stated that the budget assigned to Hybrid Threats will be invested in the establishment of an Hybrid Warfare Cell. At the time of the interview the foreseen seize of the Cell was not clear, nor what this cell will be tasked to do. Most likely the cell will be tasked with the coordination between Defence units dealing with Hybrid Threats or elements of it (for example Cyber Command and Military Intelligence and Security Service) on one hand, and other Governmental agencies dealing with Hybrid on the other hand.

Respondent 2 indicated that The Netherlands has not made much progress in structuring the countering of Hybrid Threats. In his directorate, several of his colleges are dealing with separate policies, he is the only one who is fulltime working on Hybrid. It is his opinion that the Netherlands does not experience a real threat. In the Baltic States, relative young

[133] GBVS, p. 7.

democracies with lots of ethnic Russians, with geographical borders with Russia and within close range of her military power, this threat is much more urgent than in the Netherlands.

All three respondents indicated that they were more or less the full capacity of their ministries, tasked to deal with Hybrid Threats[134].

The Joint Framework called for the establishment of new counter-Hybrid organisations like the CoE and the Hybrid Fusion Cell. These organisations are operational, and the Netherlands does participate in them. Those are no organisational elements established by the Netherlands, but participating in them shows that the importance is recognised.

Especially the efforts by the CoE are appreciated by the respondents. According to respondent 1 it has helped to connect experts from the member states with each other and has improved the exchange of information amongst countries. It has also helped to raise awareness on the concept in the Netherlands. And even though he sees significant progress, it is his opinion that the awareness of Hybrid Threats, both on the national and the international level, is not yet sufficient and should be raised even more.

Respondent 2 appreciates the efforts by the CoE to collect best practises, to educate the members and stimulate learning. He also sees an increase in the exchange of information on the international level, which has triggered the awareness process on the national level. According to respondent 2 the CoE certainly has added value, not only on the international level, but also the national awareness and commitment has been raised due to the activities deployed by the CoE.

For the indicator: national or international Organisational elements dealing with Hybrid Threats are (being) established, one piece of hard evidence can be found: the military is working on the establishment of a Hybrid Cell. The GBVS connects individual policies and comes close to policy on Hybrid Threats, but for the GBVS is explicitly stated that there will be no separate structures for the implementation. The Netherlands seems to be reluctant in creating own organisations, but it apparently does acknowledge the value of coordination and cooperation. When international organisations are created (like the CoE and Fusion Cell), the Netherlands does participate in them.

[134] For Defence this situation will be changed once the new Hybrid Cell becomes operational.

6.5 INDICATOR: NATIONAL OR INTERNATIONAL COORDINATION STRUCTURES ON HYBRID THREATS ARE (BEING) ESTABLISHED.

In the 3 National Budgets, no evidence can be found that coordination structures are established. Since all 3 hardly mention the concept of Hybrid Threats, no policies can be found and no budgets are assigned, this finding was expected.

On the national level there are no real indicators that new coordination structures are established. As we have seen in the previous indicators, for new initiatives like the one common approach against Unwanted Foreign Influence (as described in GBVS), is explicitly stated that no new structures will be set up. The letter on Unwanted Foreign Influence is written on behalf of Defence and Foreign Trade and Development, and is signed by the ministers of Justice & Security and Home Affairs. This shows a coordinated approach. But that by itself is not new. To take a random example, already in 2000, 2 years before the term Hybrid Warfare was mentioned for the very first time, the parliament was informed on the situation in Former Yugoslavia through a letter from the Prime Minister and the ministers of Foreign Affairs and Defence[135]. The sole fact that the subject is addressed in a coordinated way cannot been seen as evidence for the existence of a new structure.

Respondent 1 stated that his department has a coordinating role between the Dutch ministries. In case they recognise Hybrid Threats, they are capable of bringing the threat under attention of other ministries through regular decision- and crisis management structures, so a joint approach can be chosen. There was no statement that there is a special script or procedure for this, which suggests that this coordination is done on ad-hoc basis rather than in a structured way. The mentioned structures have been in place for quite some time and are no new structures especially established to counter Hybrid Treats. The interview did clarify that the experience and expertise to get in touch with other ministries has improved over the last years and that the crisis management procedures are under reconstruction.

Respondent 2 stated that when the Director of the security branch has bilateral meetings with his international colleagues, he frequently addresses the topic Hybrid Threats. But he also indicated that these meetings are on ad-hoc basis and are not part of a structured way of mutual consultation.

[135] De situatie in voormalig Joegoslavië, Tweede Kamer, vergaderjaar 1999–2000, 22 181, nr. 310, Den Haag, 22 maart 2000. https://zoek.officielebekendmakingen.nl/kst-22181-310.html

The international arena shows more structured activities, in which the Netherlands participates. As indicated in the Joint Framework, an international group, called the Friends of the Presidency, was established. This group has, according to respondent 1 and 2, challenged the nations to dedicate more effort to Hybrid Threats and "forced" the nations to assign national Points of Contact for the EU when addressing policies on Hybrid Threats. This structure helped to accelerate Dutch awareness on, and commitment to, Hybrid Threats. The Netherlands also participated in PACE 17/CMX17, the joint EU-NATO exercise. Exercises are meant to train people and test procedures and are by themselves no structures. Since it is the intention to hold such exercises annually, I consider them as a structured way of addressing a topic.

Participation in these international driven structures shows that the Netherlands finds it important to join the international conversation on Hybrid Threats. Evidence that comparable national structures are established could not be found. Respondent 1 indicated that new players have joined the conversation in the last few years. The Ministry of the Interior and Kingdom Relations has gotten more involved, primarily on the subject Disinformation. The EU initiative "EUvsDisinformation[136]", is part of a campaign to better forecast, address and respond to pro-Kremlin disinformation. The 'EU versus Disinformation' campaign is run by the European External Action Service East Stratcom Task Force. The campaign was launched as one of the actionable items in the Joint Framework. Unfortunately the site accidentally marked certain Dutch news items as fake news, which created significant turmoil within the Dutch press and parliament. The parliament even asked the minister of the Interior to take action to abolish this site[137]. This commotion has linked the ministry of the Interior to JenV in the context of Hybrid Threats.

For the indicator: National or international coordination structures on Hybrid Threats are (being) established, no new national structures could be found. Existing crisis management structures have improved over the years, but that progress cannot be directly linked to Hybrid. On the international level, the Netherlands does participate in initiatives by the EU. Thus underlining the importance of an international approach, and indicating that Hybrid Threats should primarily be dealt with in an international context.

[136] https://euvsdisinfo.eu/

[137] gewijzigde motie van de leden Kwint en Yesilgözzegerius ter vervanging van die gedrukt onder nr. 286, Tweede Kamer, vergaderjaar 2017–2018, 21 501-34, nr. 290, https://zoek.officielebekendmakingen.nl/kst-21501-34-290.html and; Brief van de minister van binnenlandse zaken en koninkrijksrelaties, Tweede Kamer, vergaderjaar 2017–2018, 21 501-34, nr. 294, https://zoek.officielebekendmakingen.nl/kst-21501-34-294.html

6.6 FURTHER REMARKS BY THE RESPONDENTS.

Not all the statements made by the respondents could be directly linked to one of the indicators. But since they do contribute to the overall picture, these remarks are mentioned in this section.

All 3 respondents indicated that Hybrid is a "buzzword", which is used in a flexible way to address security issues. The exact meaning of the concept is not that important. The core notion of the concept is shared by a lot of stakeholders, making it possible to discuss the essential elements and share best practises within large communities (such as the EU). And since the boundaries are not fixed, there is enough manoeuvring space for each stakeholder, preventing a stalemate over details and political sensitive issues.

All 3 respondents indicated that the fact that the EU does pay serious attention to Hybrid Threats (Joint Framework and annual reporting) has helped to get more attention for it on a national level. Also the options to discuss the subject on an international level have improved. According to respondent 1, the awareness needs to be raised even more, both in the Netherlands as in partner countries, in order to get appropriate policies and actions.

Neither of the respondents was able to indicate whether the Joint Framework has led to more structured international coordination (2 respondents had served less than 1 year on their post). Security has many faces and policies. There have always been many fora in which (parts of) security was discussed. It is hard to judge whether there is an increase in coordination. What can be noticed is that Hybrid has found its place on the agenda in many security fora.

7 CONCLUSION AND DISCUSSION

7.1 CONCLUSION

7.1.1 The extent to which the EU initiatives on Hybrid have influenced the Dutch approach is very limited.

The EU policy has not led to a Dutch national policy on the topic, nor has the term Hybrid Threat been placed on the policy agenda of the 3 examined ministries. Furthermore, existing policies on aspects like counterterrorism and cyber have not been updated in order to create synergy, as advocated by the EU. National crisis management is done through existing organisational elements and coordination structures. The crisis management procedures are under reconstruction, but only the future can tell whether they will become more Hybrid Threat orientated. Only the Ministry of Defence has allocated funds to establish a dedicated new organisational element to deal with hybrid issues. The Netherlands does participate in the new organisations and structures, like the CoE, the Fusion Cell and the Friends of the Presidency, established by the EU as advocated by the Joint Framework. This will influence the Netherlands, but to what extent could not be measured.

7.1.2 How to explain the limited influence.

A clear explanation is hard to find, there are no declined propositions for setting up a policy or organisation. The minutes on the associated decision making process could have shed a light on why it was rejected. From the examined documents and the interviews the following reasons can be subtracted.

- Hybrid Threat is seen as a buzzword which helps to get attention to security issues and improve awareness on threats surrounding us. In the Netherlands it is seen as an effective accelerator, rather than a fixed concept.
- The Netherlands does not experience a real threat by one actor that has the strategic objective to undermine, or even overthrow, the Dutch society.
- Hybrid Threats are difficult to recognise. Individual threats, like terrorism, cybercrime and disinformation, are much more tangible and the effects are felt by the population. Policies to counter these threats do already exist and intensifying those policies is considered to be sufficient to deal with the threats that are experienced.

- The Netherlands doesn't feel threatened by Hybrid Threats but recognises the potential of the concept against partner nations like the Baltic States, it seems to think that those threats are best dealt with by the international community.

To reach back to the assumption as stated in chapter 1.4.: if the Netherlands is working on an own national policy on Hybrid Threats, and that this policy reflects the actionable items as proposed by the EU, the Netherlands acknowledges Hybrid Threats to be real threats *and* considers the EU initiatives to be meaningful. There is no clear sign that the Netherlands is working on an own policy, basically *because* Hybrid Threats are not considered to be real. Concerning the concept of Hybrid Threats, the Netherlands appears to be hopping on two thoughts. The threats are not taken serious enough to come up with an national approach. But the concept is not completely dismissed. The Netherlands does participate in initiatives taken by the EU, thus acknowledging that there are threats, *and* that at least parts of the EU initiative is seen as useful.

7.2 DISCUSSION

The discussion on Hybrid Threats seems to have 2 major aspects; an academic and a societal and administrative one.

On the academic site, a lot has been written on the concept. It is of course the prerogative of scholars to have their own opinion and views, and add new information and use different angles of approach on a subject. But all the discussion has not led to any form of convergence of the concept, the opposite seems to be happening. It is of course mighty interesting to analyse all the things that can threaten a society and how they can be used against an opponent, like Cullen and Reichborn-Kjennerud did (chapter 2.6), making clear that the threat can come from many sides and that the whole society can be targeted. To counter such threats, calls for an all-embracing approach can be heard (something referred to as whole-of government or whole-of-society). The CoE states that "understanding the threat, understanding one's own system and its vulnerabilities, directing resources to address the vulnerabilities, and organising a reliable, all-domain situational awareness unlock the distributed domain-specific detection and response mechanisms." And if that is not enough, also an effort should be made to "pinpointing of vulnerabilities that may be hiding on organisational borderlines, out-of-date pieces of legislation, insufficient mandates for agencies and authorities, and confusing or completely missing processes for response mechanisms that involve many actors.[138]" If you make a concept that complex, is it still a concept, or has it become a collection bin of security related notions? Too broad and vague to help you solve a problem, but great for cherry-picking policy-entrepreneurs. I have read the following sentence many times during the master CSM, and I hated it, but now I will use it myself: if you try to describe everything you end up describing nothing.

On the societal and administrative site, the vagueness and broadness of the concept leads to other problems. As we have seen the Netherlands does not feel a serious threat form another state actor that tries to overthrow our society. If you take the cynical approach, one might say that we are so ignorant that we do not see the evil in the world around us. When choosing a more optimistic view, one can argue that we are so well organised that we are no viable target for a foreign country. The Netherlands is a wealthy state, has a strong democracy, a solid social welfare system, good health facilities, a flourishing economy, freedom of speech and freedom of press, high technological standards, almost unlimited access to internet, a decent military force, well organised intelligence services[139] and is deeply embedded in trade and defence alliances like the EU and NATO. So, except for some individual terrorists or cyberbullies that annoy us, who can hurt us? Do we indisputably need the integrated Hybrid approach to stay safe in the future, or is the approach based on individual policies good enough?

The problem every decision maker is confronted with, is that it is impossible to tell what will happen in the future and what cunning plans are made by non-allied countries that can threaten our "perfect" society. We can notice all kind of events, like cyberattacks, support to terrorist groups, spreading of disinformation, investment in (re)armament, the foreign take-over of critical infrastructure, the use of essential goods (like gas and oil) as means of pressure. But how can you tell that these actions are all connected and have a strategic objective? And what is that objective? And has the opponent the intention to go all the way, even if it takes years to achieve it? Despite all the efforts of the intelligence services, I do not believe that anyone can predict what will happen. Of course it is important to keep monitoring those activities, to search for connections and to come up with scenario's, to make sure that we are aware how dangerous the world is and to prepare to defend us. Intelligence does play a crucial role in that. But it still does not provide prove for the other's intentions. Even in the

[138] Both quotes taken from Cederberg, Eronen and Mustonen, Regional Cooperation to Support National Hybrid Defence Efforts Hybrid, CoE Working Paper 1 • October 2017, p.7.

[139] No offence to the hard working people in the military and intelligence services, but on a global scale the Dutch capabilities are of course very limited.

Cold War "neither UK nor US intelligence was ever able to develop covert sources as its own transparent window on to Soviet policies and policy-making[140]".

Those responsible to decide whether to continue to focus on individual threats, or that the moment has come that a shift to the wholistic approach, carry a heavy load. All they can be sure of is that the information they base their decision on is incomplete, and only history can tell whether they have made the right choice. But since the contemporary, individual policies seem to do the job and provide security, or at least provide the comfortable feeling that we are not threatened, there does not seem to be a reason to change the approach.

Perhaps van Puyvelde is right (see chapter 3.1) when he advices decision-makers to focus on the threats they are confronted with, and to look for connections between these threats, and to forget all about Hybrid Warfare.

[140] Michael Herman, What Difference Did It Make? Intelligence and National Security Vol. 26, No. 6, 886–901, December 2011, p. 894.

8 ABBREVIATIONS

ACT	Allied Command Transformation
Bi-SC	Bi- Strategic Command
BuZa	Buitenlandse Zaken (Ministry of Foreign Affairs)
CA	Comprehensive Approach
CBRN	Chemical, Biological, Radiological and Nuclear
CoE	Centre of Excellence
EEAS	European External Action Service
EU	European Union
EUGS	European Union Global Strategy
GBVS	Geïntegreerd Buitenland en Veiligheid Strategie (Integraded Foreign and Security Strategy)
IDF	Israel Defence Forces
IPCR	Integrated Political Crisis Response
ISIS	Islamic State of Iraq and Syria
IVS	Internationale Veiligheidstrategie (International Security Strategy)
JenV	Justitie en Veiligheid (Ministry of Justice and Security)
MCCHT	Military Contribution to Countering Hybrid Threats
MFP	Multiple Futures Project
MinDef	Defensie (Ministry of Defence)
MPECI	Military, Political, Economic, Civilian and Informational
NCTV	Nationaal Coordinator Terrorismebestrijding en Veiligheid (National Coordinator Counter Terrorism and Security)
NATO	North Atlantic Treaty Organisation
OSCE	Organisation for Security and Cooperation in Europe
PMESII	Political, Military, Economic, Societal, Informational and Infrastructure
SU	Soviet Union.
UN	United Nations
US	United States

9 References

9.1 Authors

Abbott, Katie; "Understanding and Countering Hybrid Warfare: Next Steps for the North Atlantic Treaty Organization", University of Ottawa, March 23, 2016.

Bartkowski, Maciej; Nonviolent Civilian Defense to Counter Russian Hybrid Warfare, The Johns Hopkins University Center for Advanced Governmental Studies, March 2015.

Bartles, Charles K.; Getting Gerasimov Right, Military Review, Jan-Feb 2016

Binnendijk, Hans and Johnson, Stuart E.; Transforming for Stabilization and Reconstruction Operations, Center for Technology and National Security Policy, National Defense University, Washington, DC, 2004.

BI-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats, 1500/CPPCAM/FCR/10-270038 5000 FXX 0100/TT-6051/Ser: NU0040, August 2010.

Biscop, Sven; Hybrid Hysteria, Security Policy Brief no. 64, June 2015.

Bond, Colonel Margaret S.; Hybrid war: a new paradigm for stability operations in failing states, U.S. Army War College, 30 Mar 2007.

Cecire, Michael; The Russian invasion of Ukraine, Foreign Policy Research Institute, March 2014.

Cederberg, Eronen and Mustonen; Regional Cooperation to Support National Hybrid Defence Efforts Hybrid, CoE Working Paper 1 • October 2017.

Charap, Samuel; The Ghost of Hybrid War, Survival, vol. 57 no. 6, December 2015–January 2016.

Coalson, Robert; Top Russian General Lays Bare Putin's Plan for Ukraine, Huffpost, Sept 2014.

Cullen, Patrick J. & Reichborn-Kjennerud, Erik; "Countering Hybrid Warfare (CHW) Analytical Framework", Multinational Capability Development Campaign (MCDC), 1 October 2016.

Cullen, Patrick J. & Reichborn-Kjennerud, Erik; "Countering Hybrid Warfare (CHW) Baseline Assessment", Multinational Capability Development Campaign (MCDC), 1 October 2016.

Drent, Margriet et al; New Threats, New EU and NATO Responses, Netherlands Institute of International Relations Clingendael, July 2015.

Fiott, Daniel et al; The common security and defence policy: national perspectives, Egmont Paper 79, May 2015.

Flyvbjerg, Bent; Five Misunderstandings About Case-Study Research, Qualitative Inquiry Volume 12 Number 2 April 2006.

Galeotti, Mark; The 'Gerasimov Doctrine' and Russian Non-Linear War, In Moscow's shadows, July 2014.

Galkins, Kaspars; NATO and hybrid conflict: unresolved issues from the past or unresolvable threats of the present?, NAVAL POSTGRADUATE SCHOOL, September 2012.

Giles, K. "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power", Chatham House Research Paper, London, RUSI, 2016.

Gill, Terry D. and Ducheine, Paul A. L.; Anticipatory Self-Defense in the Cyber Context, International Law Studies, 2013.

Herman, Michael; What Difference Did It Make? Intelligence and National Security Vol. 26, No. 6, 886–901, December 2011.

Herta, Laura-Maria; Hybrid Warfare – a form of asymmetric conflict, International Conference Knowledge-Based Organization Vol. XXIII No 1 2017.

Hoffman, Frank G.; Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies Arlington, Virginia December 2007.

Hoffman, Frank G.; 'Hybrid Threats': Neither Omnipotent Nor Unbeatable, FPRI, July 2010.

IONIȚĂ, Craișor-Constantin; Is hybrid warfare something new?, Strategic Impact No. 4/2014.

Kalpokas, Ignas; Influence Operations: Challenging the Social Media – Democracy Nexus, Sais Europe journal of global affairs Volume 19.

Kaspoglu, Can; Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control, NATO research paper 121, November 2015.

Kenan, George; The inauguration of organized political warfare, Policy Planning Staff Memorandum, May 1948.

Kumar, Ranjit; Research methodology a step-by-step guide for beginners 3rd edition, SAGE Publications Ltd, 2011.

Lasconjarias, Guillaume and Larsen, Jeffrey A.; Introduction: A New Way of Warfare, in Guillaume Lasconjarias and Jeffrey A. Larsen, NATO's Response to Hybrid Threats, NATO Defense College, Forum Paper 24, 2015.

McCulloh, Timothy B.; The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?, JSOU Report 13-4, The JSOU Press MacDill Air Force Base, Florida 2013.

Mearsheimer, John J.; Back to the Future: Instability in Europe after the Cold War, International Security , Vol. 15, No. 1 (Summer, 1990).

Münkler, Herfried; Hybrid Wars. The Dissolution of the Binary Order of War and Peace, and Its Consequences, Ethics and Armed Forces, Issue 2015/2.

NATO ACT, Multiple Futures Project, navigating towards 2030, April 2009.

Nemeth, William; Future War and Chechnya: a Case for Hybrid Warfare, Naval Postgraduate School, June 2002.

O'Connell, Mary Ellen; Myths of Hybrid Warfare, in Ethics and Armed Forces, Issue 2015/2.

Pawlak, Patryk; Understanding hybrid threats, European Parliamentary Research Service, June 2015.

Pawlak, Patryk; Countering hybrid threats: EU-NATO cooperation, European Parliamentary Research Service, March 2017.

Popescu, Nicu; Hybrid tactics: Russia and the West, European Union institute for Security Studies, October 2015.

Praks, Henrik; Hybrid or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics The Case of Estonia, in: Guillaume Lasconjarias and Jeffrey A. Larsen, NATO's Response to Hybrid Threats, NATO Defense College, Forum Paper 24, 2015.

Puyvelde, Damien van; Hybrid War – does it even exist? NATO review magazine, 2016.

Samadashvili, S.; Muzzling the Bear, Strategic Defence for Russia's Undeclared Information War on Europe, Wilfried Martens Centre for European studies, 2014.

Starink, Laura en Smeets, Hubert; Ruslands machtspolitiek: voor staat, taal en kerk, in Magazine Nationale veiligheid en crisisbeheersing, Thema Hybride dreigingen, 14e jaargang 2016 nr. 5/6.

Tenenbaum, Élie; Hybrid Warfare in the Strategic Spectrum: An Historical Assessment, in Guillaume Lasconjarias and Jeffrey A. Larsen, NATO's Response to Hybrid Threats, NATO Defense College Forum Paper 24.

Uzieblo, "Jan Jakub.; United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats", EU Diplomacy Papers 5/2017.

Vaske, Gertrud; Hybrid Warfare – A Crisis on Our Doorstep, in Ethics and Armed Forces, Issue 2015/2.

Weitz, Richard; Countering Russia's Hybrid Threats, Diplomaatia No. 135 • November 2014.

Whetham, David "Hybrid Warfare" and the Continuing Relevance of the Just War Tradition in the 21st Century, Ethics and Armed Forces, Issue 2015/2.

Wijk, Rob de; Hybride dreigingen, in Magazine Nationale veiligheid en crisisbeheersing, Thema Hybride dreigingen, 14e jaargang 2016 nr. 5/6.

Yin, Robert K.; Case Study Research, 3rd edition, Applied social research methods series Vol 5, Sage publications, 2003.

9.2 EU PUBLICATIONS

COM(2017) 610 final, Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, Brussels, 18.10.2017.

EEAS(2015) 731, Food-for-thought paper "Countering Hybrid Threats", European External JOIN (2013) 30 final, The EU's comprehensive approach to external conflict and crises, Brussels, Dec.2013.

European Parliament, EPP Group, The supreme art of war is to subdue the enemy without fighting, Brussels, 19 April 2016.

JOIN(2016) 18 final, Joint Framework on countering hybrid threats; a European Union response, Brussels, Apr.2016.

JOIN(2017) 30 final, joint report to the European parliament and the Council

on the implementation of the Joint Framework on countering hybrid threats - a European Union response, Brussels, 19.7.2017.

JOIN(2018) 14 final, on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018, Brussels, 13.6.2018.

JOIN(2018) 16 final, Increasing resilience and bolstering capabilities to address hybrid threats, Brussels, 13.6.2018.Action Service, May 2015.

9.3 DUTCH DOCUMENTS

Beleidsdoorlichting Defensie, brief van de ministers van defensie, van buitenlandse zaken, voor buitenlandse handel en ontwikkelingssamenwerking en van justitie en veiligheid, Den Haag, 28 maart 2018.

Brief ongewenste buitenlandse inmenging, Nationaal Coördinator Terrorismebestrijding en Veiligheid, kenmerk 2223363, 16 maart 2018.

Brief van de minister van binnenlandse zaken en koninkrijksrelaties, Tweede Kamer, vergaderjaar 2017–2018, 21 501-34, nr. 294.

De situatie in voormalig Joegoslavië, Tweede Kamer, vergaderjaar 1999–2000, 22 181, nr. 310, Den Haag, 22 maart 2000.

Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022, Wereldwijd voor een veilig Nederland, 14-05-2018.

Gewijzigde motie van de leden Kwint en Yesilgözzegerius ter vervanging van die gedrukt onder nr. 286, Tweede Kamer, vergaderjaar 2017–2018, 21 501-34, nr. 290.

Internationale Veiligheidsstrategie, Veilige Wereld, Veilig Nederland, 21-06-2013.

Rijksbegroting Veiligheid en Justitie, Tweede Kamer, vergaderjaar 2014–2015, 34 000 VI, nr.2

Rijksbegroting Justitie en Veiligheid, Tweede Kamer, vergaderjaar 2017–2018, 34 775 VI, nr.2

Rijksbegroting Buitenlandse Zaken, Tweede Kamer, vergaderjaar 2014–2015, 34 000 V, nr. 1

Rijksbegroting Buitenlandse Zaken, Tweede Kamer, vergaderjaar 2017–2018, 34 775 V, nr. 1

Rijksbegroting Defensie, Tweede Kamer, vergaderjaar 2014–2015, 34 000 X, nr. 2

Rijksbegroting Defensie, Tweede Kamer, vergaderjaar 2017–2018, 34 775 X, nr. 1