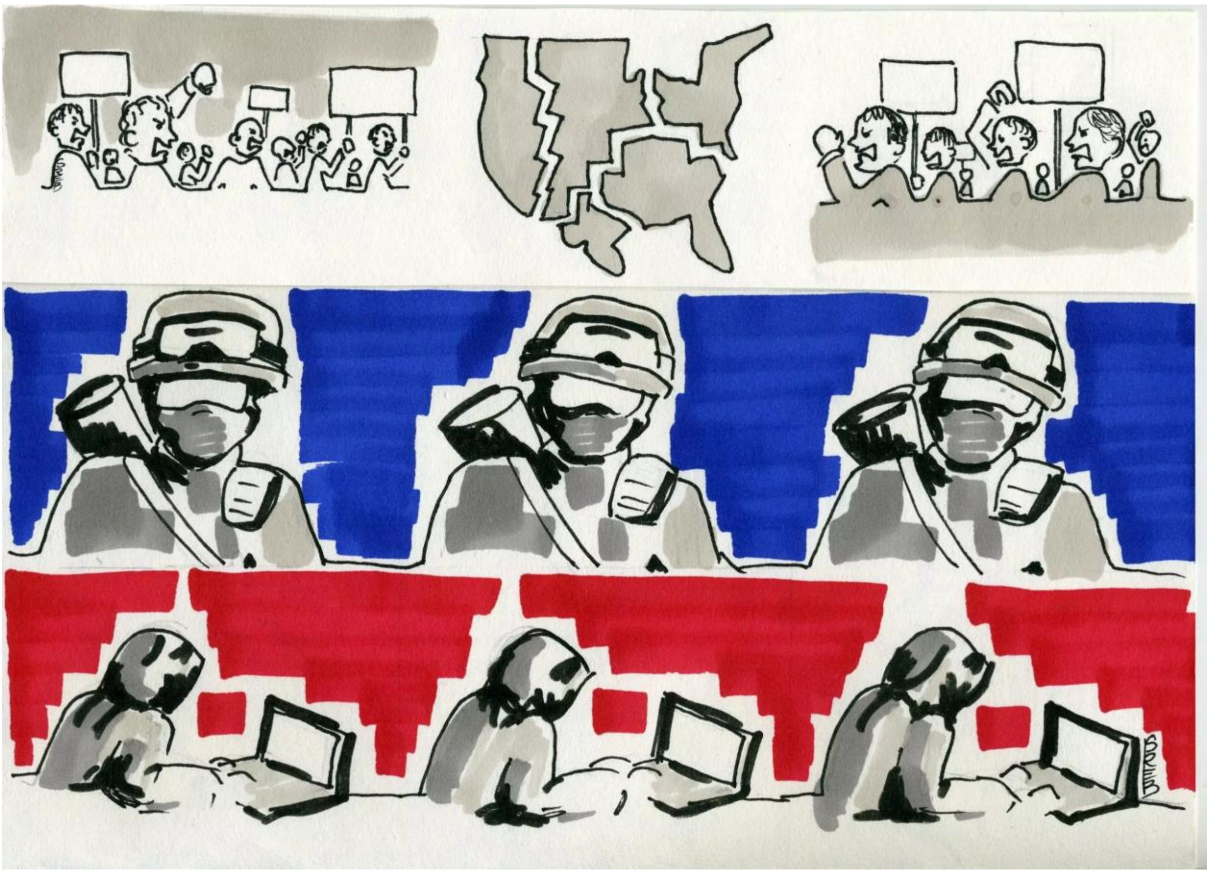
Leiden University Master Thesis International Relations

# Hybrid War and Peace

## Or Death by a Thousand Cuts

**Maxim Doorn**

S1403958



Specialization: Conflict in the Modern Era

Supervisor: Dr. L. Milevski

Word Count: 14930

Date: 05-07-2019

# Table of Contents

# 1. Introduction

In March 2014, the heart of the European continent endured a warlike situation for the first time since over a decade, causing a crisis on Ukrainian soil that is still ongoing today. This crisis ignited popularity around the term "Hybrid Warfare". In the final weeks of 2013 and the first weeks of 2014 mass protests took place in Ukraine, which would eventually lead to the ousting of the reigning president. The protests, now known as the Maidan revolution, took place after president Yanukovych decided not to sign an association agreement with the European Union, but instead signed a new trade-treaty and loan with the Russian Federation. This decision initially provoked (mostly student) protests in December 2013, which lead to a full-fledged revolution by February 2014. While the revolution itself sparked much violence leading to a death toll of almost 130 people, the violence did not end with the revolution's success, as civil unrest and eventually war spread to the Southern and Eastern regions of Ukraine causing a crisis which still continues today.

At the end of February, alongside cyber operations targeting Ukrainian media and politicians, pro-Russian uniformed men began taking the streets on the Crimean peninsula, inciting riots and taking over government buildings. Although the Russian government initially denied that these militants without insignia, also known as "little green men", were Russian soldiers, claiming them to be local self-defence forces, it was later admitted that they were in fact forces belonging to the Russian Federation. Halfway through March, a self-proclaimed pro-Russian government announced a referendum to join the Russian Federation, and by March 18th Russia annexed Crimea, with little bloodshed. This ambiguous and multi-dimensional operation was organized in way 'the West' had not expected and was not prepared for, and is now often used as a prime example of what is called (Russian) hybrid warfare.

While the situation in Crimea remained relatively calm after the peninsula was annexed by the Russian Federation, the ongoing war in the south-eastern parts of Ukraine continues to take lives on a daily basis. Although this region is allegedly ruled by self-proclaimed pro-Russian separatists, many politicians blame Russia for ruling it from the shadows.

The way Russia has acted during and after the Maidan revolution, annexing Crimea, and with regard to the ongoing war in Eastern Ukraine, is often referred to as hybrid warfare. The strategies that have been applied during the Ukraine crisis are both in the media and in research often mentioned as being new, pointing at a changing nature of warfare. Not only the term *hybrid warfare*, but also the concepts of "new-generation warfare", "gray-zone conflicts", "competition short of conflict", and "active measures" can often be encountered when looking into the situation in Ukraine. While Ukraine is not the only context in which these concepts can be encountered, it is often referred to as the leading and best example. To further complicate the situation not only concepts like *new-generation warfare*, *gray-zone conflicts* and *hybrid warfare* are encountered when looking into what is currently going on in Ukraine. Terms like *proxy war*, *civil war*, *asymmetric war*, and *interstate war* are also often encountered. Most of the terms mentioned above are either interconnected or share elements making it harder to pinpoint the most relevant concept for the situation.

## 1.1. Research Question

The concept of hybrid warfare, regarding how 'the West' perceives Russia to employ it, is the core subject of this thesis, taking into account both the advantages and disadvantages of using such a term, explaining its specific elements when comparing it to other types of warfare, and looking into the politicisation of the term. Since many authors are of the opinion that hybrid warfare currently lacks a general theory which properly distinguishes it from other types of warfare, and that could serve to frame it in a meaningful manner, this thesis will contribute to a critical understanding of the current security environment with regards to perceived Russian hybrid threats. As the concept of hybrid warfare has grown up to the extent where it can encompass virtually anything relating to conflict, this thesis will emphasize the cyber domain, alongside (mis)information operations as these can be considered as some of the most unconventional concepts in contemporary warfare.

Not all opinions on the concept of hybrid warfare will or can be taken into account, since the subject itself remains very broad, and is often disputed. Studying the notion of hybrid warfare is relevant, for it is not only important for academics and military strategists, but can also be useful for policy makers and citizens in providing them with an understanding on the changing character of warfare. For the military, in order to organize and equip itself with the capabilities that are needed to achieve its objectives, it is important that the terms in use are able to properly describe the challenges it is facing. In order to do so, a shared understanding between military, policy makers and the broader public on developments in the current state of warfare is of importance (Chambers 4). This thesis will summarize the discourse regarding the perception of Russian hybrid threats in the West, emphasizing the issues of using a broad umbrella term such as hybrid warfare with regards to Russia in the contemporary security environment, explaining the effect of the politicisation of the term alongside the challenges the term faces. Due to the lack of consensus regarding the term, the politicisation and the broadness, this thesis will plead for the separate analysis of cyberwarfare and information warfare beside new notions of warfare which include both military and non-military means. As such this thesis will set out to answer the question: Is hybrid warfare a viable term with regards to Russia in the current security environment?

## 1.2. Methodology and Structure of this Thesis

This thesis is based on literature research of both primary and secondary sources from academics, policy-advisors, intelligence agencies, military personnel, and media. In order to explain the challenges of the current security environment with regards to perceived Russian 'hybrid threats', some of the most commonly encountered concepts relating to this topic will be summarized (Chapter 2). The main concepts of hybrid warfare (in Frank Hoffman's definition), new-generation warfare, and gray-zone warfare will be treated in Chapter 3. While discussing these concepts and theories, we will encounter references to 'the Gerasimov doctrine' and 'unrestricted warfare', which will be discussed in more detail. The summary of these topics is meant to show gaps in understanding, and pin-point challenges to the current popular theoretical notions.

In order to provide a clearer understanding regarding the political-military challenges faced by Western academics, politicians and military leaders, a brief overview of Russian military thought regarding hybrid warfare and information operations (although mostly gathered from secondary sources) will be provided in Chapter 4. The difference encountered between Western and Russian theories is used to provide a better understanding of the politicisation of the concept of (Russian) hybrid warfare (Chapter 5). As the literature review will show, there is a strong case to be made against the claimed 'novelty' of most of these concepts. Although the concepts themselves may not be new, they do provide the international community with a new set of challenges which are mostly of technological nature. As an important manifestation of this, the cyber domain will be looked into in Chapter 6. In the concluding Chapter 7 it is attempted to summarize the findings and to reflect on the research question formulated earlier in this Chapter 1.

# 2. The Changing Nature of Warfare – a Conceptual Framework

## 2.1. War and Warfare

Both war and warfare are arguably as old as humanity itself. It is not uncommon for historians to refer to casualties from war over the centuries when analysing changes in its practice. When studying and defining a change in the nature of warfare, it is important to mention what the change relates to. For example: a changing number of casualties over the years can be used to indicate a change in nature, as it can be an expression of new methods, tactics, and/or equipment, etc. While the concepts of war and warfare appear to be clear to the common public at first glance, in depth knowledge of the topics involved often appears to be absent.

The terms war and warfare are often used interchangeably. While in a 'common' conversation this might work, for both policy makers and academics alike it is important to distinguish between the two. The term war can be used in a variety of ways. Governments can be fighting a war on drugs, companies can be in a price war, and groups of people (states and/or non-state actors) can be at war with each other. The latter concept of war, being a state of armed conflict between two or more countries or groups within a country, is relevant for this paper. Warfare, although in ordinary conversations often used interchangeably with war, refers to the actual act of fighting a war, including the setting and methods that are used, e.g.: naval warfare.

## 2.2. War and Armed Conflict

Not only war and warfare are often used as synonyms, as the term (armed) conflict can also be encountered as a (false) synonym for war. When either researching war, and the idea of its changing nature, fighting wars, or being involved in writing policies that concern war, it is of importance to distinguish between the concepts of war and conflict, or better said, to be aware of the fact that they do not always mean the same. Fixed definitions of the concepts of war and conflict appears to be absent, but knowledge about a variety of meanings is useful in deciphering the hidden message in certain claims. One relatively in-depth definition of armed conflict is provided by the Uppsala Conflict Data Program (UCDP): "a contested incompatibility that concerns government and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths in a calendar year" (Pettersson, Therése and Eck 16). While an armed conflict according to the Uppsala definition requires a minimum of 25 battle-related casualties a year, it is often considered to evolve into a war once it leads to a thousand or more casualties annually according to the UCDP. While this distinction might not be of much significance to many citizens, it is of importance in order to research trends concerning international (and/or intra-state) relations and the current security environment, both nationally and internationally. This distinction is of importance when researching war and warfare in contemporary times. When analysing historical figures concerning war over the centuries it can be seen that the number of (inter-state) wars has declined, whilst the number of conflicts has gone up in the last century.

Defining war as an armed conflict between multiple groups that directly, through violence (thereby not taking into consideration the effects of lack of food or medicine, or displacement), causes at least 1000 deaths annually, as defined by the UCDP and SIPRI (Stockholm International Peace Research Institute), appears to be straightforward. In the last decades however, many forms of warfare that do not necessarily involve human casualties (or even physical destruction) have emerged, complicating the concept of war.

## 2.3. The Labelling of Wars

When going further in depth on the topics of conflict, war and warfare, one has to look into a great variety of aspects. As Dosse states: “War has a unique nature but several faces, which are usually categorized in the form of an adjective—thus, war or warfare can be described as just, necessary, regular, irregular, interstate, asymmetric, civil, humanitarian, extermination, total, limited, nuclear, conventional, movement, electronic, etc.” (Dosse 1). The labelling of wars has both advantages and disadvantages. For the military to prepare and effectively act in war, it has to distinguish the type of war it will be involved in, being interstate or intrastate, conventional or asymmetric, on land, air or sea.

A downside to the labelling of wars can be found in the United States of America’s campaign in Iraq. Donald Rumsfeld, who was US Secretary of Defense between 2001 and 2006, forbade the usage of the term ‘insurgency’ to describe the hostile events in Iraq. If the hostilities encountered in Iraq after the US invasion in 2003 would be labelled as insurgency, it would invalidate the neoconservative political assumptions and rhetoric that underpinned the invasion. As Milevski puts it: “In such circumstances, strategy is beholden to a political debate about labels and is prevented from serving the desired policy. Use of a label becomes of greater concern than pursuit of success in the war” (Milevski 39). Had the situation in Iraq been called an insurgency, then the United States Armed Forces active in Iraq would have been able to apply other tactics. This example illustrates the role and impact of politicisation of the terms involved.

# 3. Hybrid Warfare – a Literature Review

## 3.1. Hybrid Warfare According to Frank Hoffman

Over the past few decades there has been much debate and writing about the evolution of modern warfare in the post-Cold War world. A changing nature of warfare has often been mentioned, and several authors have claimed a “revolution in warfare”. Conventional and/or big wars have decreased and have mostly ceased to exist, with only two conventional interstate wars taking place since the turn of the millennium; in 2003 when the United States invaded Iraq, and in 2008 when Russia waged a 5-day war against Georgia. Smaller intrastate wars or conflicts, often with an irregular aspect, have however increased in number over the past century.

According to Frank Hoffman it is too simplistic to merely classify conflict and war in categories like conventional, big, irregular or small. While countries have long prepared for either conventional threats posed by state-actors, or asymmetric or irregular tactics posed by non-state actors Frank Hoffman argues that these may no longer be separate threats or modes of war (Hoffman, *Conflict in the 21st Century* 7). Adversaries in the 21st century are likely to employ a combination of warfare types. Non-state actors mostly employ irregular forms of warfare, but can be expected to participate in conventional warfare if it serves their goals. Similarly, nation-states may engage in irregular warfare if it helps them achieve their goals. The integration and fusion of both irregular and conventional tactics by states as well as non-state actors on a single battlefield was coined as hybrid warfare by Frank Hoffman, defining wars, wherein this type of warfare is used, as follows: “Hybrid wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.” (Hoffman, *Conflict in the 21st Century* 14).

Retired Col. David Maxwell however argued before the U.S. House Armed Services Committee that hybrid warfare instead of being a new concept is merely a new name for irregular warfare, more specifically, for its subdivision of unconventional warfare (Chambers 10). The Joint Staff in Joint Publication (JP) 1-02 *Department of Defense Dictionary of Military and Associated Terms*, defines irregular warfare as “a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations,” (JP 119) and unconventional warfare as “activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area” (JP 249).

After the Maidan revolution took place in Ukraine, which was followed up by the annexation of Crimea by the Russian Federation and a still ongoing conflict in the Donbas region of the country, the term Hybrid Warfare gained popularity both in the media and in political spheres. More proponents and opponents began writing about the concept. Its definition, although lacking a consensus, appears to have changed.

In his 2014 work *On not-so-new warfare: political warfare vs hybrid threats,* Frank Hoffman states that the ongoing conflict in Ukraine challenges the traditional Western concepts of warfare. The crisis, in which the Ukrainian government fights against pro-Russian separatists, Russian ultra-nationalists, proxy fighters and likely Russian GRU (military intelligence) personnel, does not fit Western categories of 'war'. The war that is ongoing in Ukraine has aspects of various different types of war. By some it is regarded as a civil war, or possibly a proxy war. United States army General Barno, former head of combined forces command in Afghanistan, referred to the aforementioned crisis as an example of a 'shadow war'. The general notes that contemporary war is morphing beyond our current conceptions, demonstrating 'different' forms of unconventional warfare fought by masked warriors without apparent state attribution, using high tech weaponry such as SA-11 BUK SAM (surface-to-air) missile systems and T-72 tanks, subversion, and covertly receiving backing from nation-states. Besides the concept of shadow war, the term 'political warfare' has also been raised in order to describe ambiguous and nebulous conflicts that do not fit in with our current concepts of war (Hoffman, *On Not-So-New Warfare*). Hoffman argues that the term hybrid warfare does not only adequately represent the Russian action in Georgia in 2008, which by some is described as the first occasion in which large-scale cyber warfare and military engagement happened at the same time (Markoff), but that it dovetails how Russians are fighting in Ukraine. The type of warfare Russia employs in Ukraine has been categorized under many names, and although both terms "new warfare" and "political warfare" can be deemed to be partially correct, Hoffman argues that the term "hybrid" better captures its essence. (Hoffman, *On Not-So-New Warfare*). Although the West alongside the Ukrainian government had not been prepared for the tactics employed by Russia, Russian actions in Ukraine can partially be compared with the older Soviet tactics of *Maskirovka* (translated as masked warfare), and can therefore hardly be called new. Nonetheless its contemporary tactics have been evolving and incorporate more violent and lethal conventional capabilities, which are combined with tactics most often associated with terrorists or irregular means of conflict. In addition, the issue with political warfare lies in its wording. The definition states that political warfare is the use of political means, which can be combined with the employment of all means short of war, by a nation-state to achieve its objectives, with as main element the "the use of words, images and ideas" (Smith 3). This definition only partially fits Russia's actions in Ukraine (and Georgia), as it does not correspond with the heavy reliance on military means. Furthermore, the concept focuses on means short of war, which makes it questionable whether it captures the essence of warfare and can be called as such. Hybrid warfare as Hoffman puts it can be seen to apply to the multidimensional actions used in Ukraine as it combines conventional military force with irregular tactics, the employment of criminals and acts that are at times regarded as terroristic in nature.

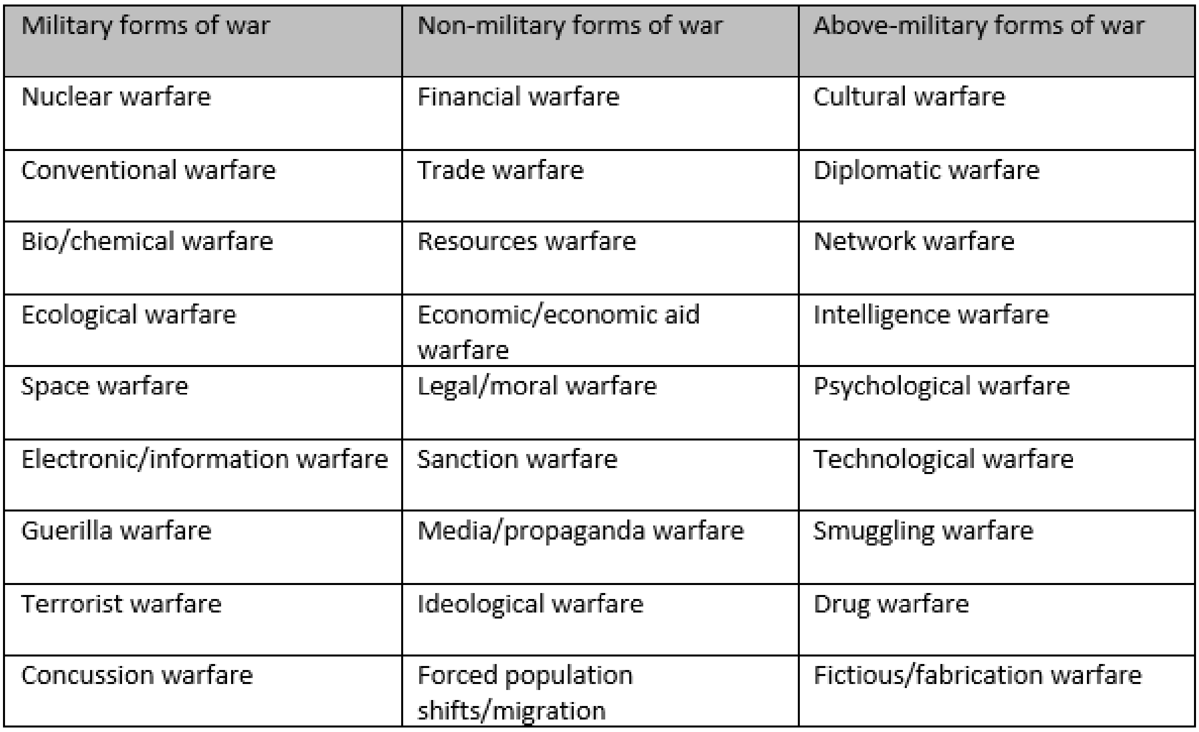
Frank Hoffman's original definition of hybrid warfare did however face a lot of critique as well. As mentioned previously, a consensus on the concept of hybrid warfare appears to be lacking, especially after the association of the concept with the crisis in Ukraine. Hoffman himself already noted that one of the issues with his concept is that it only focuses on a combination of tactics that are associated with violence and warfare, whereby it fails to capture non-violent acts such as economic, financial, misinformative, and subversive political acts. Moreover, Hoffman's hybrid warfare concept focuses solely on the operational and tactical levels (means), but is not suitable when explaining strategy (long-term plan). While Hoffman takes into account kinetic acts, which are capabilities of physical nature that focus on destroying enemy forces, others like Mark Galeotti broaden the notion of hybrid warfare by taking into account non-kinetic, and mostly non-military, acts (Hybrid, ambiguous, and non-linear 287).

Galeotti states that the tactics in use often have a more non-kinetic nature, for example information warfare, and where the warfare is of kinetic nature local actors and proxy forces are mostly deployed. As mentioned previously, these tactics are often described as 'new' forms of warfare, although they do not appear to differ a lot from Western military practices, most notably by their special forces. Galeotti writes that the tactics are not particularly new, but that the context in which the methods are applied has changed. He considers the outcome to be a form of "guerrilla geopolitics" wherein a would-be great power realizes that its ambitions are greater than its (military) resources, and therefore uses the methodologies of an insurgent in order to maximize its capabilities (Galeotti, Hybrid, ambiguous, and non-linear 283).

The non-military part of Russia's actions in Ukraine influenced what is referred to as hybrid warfare. Another term used nearly synonymously with hybrid warfare in Western circles is what Galeotti called "the Gerasimov Doctrine", basing himself on the writings of Russian Chief of General Staff Gerasimov in "*The value of science is in the foresight: new challenges demand rethinking the forms and methods of carrying out combat operations",* preceding the Ukraine crisis in 2013 (Galeotti, *The 'Gerasimov doctrine' and Russian non-linear war*). This perceived 'doctrine' allegedly fuses hard and soft power across all domains, transcending boundaries between peace and war, and relies heavily on non-military means. Although the Gerasimov doctrine is often regarded as a re-invention of, or new approach to, warfare, the idea that conflicts would become multi-dimensional and “civilianized” emerged long before the Ukrainian crisis. Chinese colonels Liang and Xiangsui foresaw a change in warfare and published a book about it in 1999 called *Unrestricted Warfare,* which was framed as a response to the overwhelming victory of the United States in the First Gulf War (Liang & Xiangsui). According to these colonels, war was no longer strictly limited to military means, but instead it had evolved to “using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means, to compel the enemy to accept one’s interests” (Bensahel). The distinction between soldier and civilian was expected to vanish, since society itself was expected to become the battlefield. The number of battlefields was expected to become “virtually infinite”, as it was predicted that both traditional and non-traditional combatants were likely to use at least 27 different forms of warfare simultaneously at any given time (Callard and Faber 63), which could include environmental warfare, cultural warfare, and legal warfare, among many other forms. The first rule of unrestricted warfare would be that there are no rules, nothing would be forbidden, which clearly transcends traditional concepts of war and peace (Bensahel).

The Colonels categorized the following terms of warfare stating that “a better means used alone will not prevail over multiple means used together” (Figure 1):

*Figure 1. Categorization of Callard and Faber’s 27 forms of warfare*



| Military forms of war | Non-military forms of war | Above-military forms of war |
|---|---|---|
| Nuclear warfare | Financial warfare | Cultural warfare |
| Conventional warfare | Trade warfare | Diplomatic warfare |
| Bio/chemical warfare | Resources warfare | Network warfare |
| Ecological warfare | Economic/economic aid warfare | Intelligence warfare |
| Space warfare | Legal/moral warfare | Psychological warfare |
| Electronic/information warfare | Sanction warfare | Technological warfare |
| Guerilla warfare | Media/propaganda warfare | Smuggling warfare |
| Terrorist warfare | Ideological warfare | Drug warfare |
| Concussion warfare | Forced population shifts/migration | Fictious/fabrication warfare |

*Source: Adapted from:* Callard and Faber, 63

With the concept of unrestricted warfare, elaborated by Callard and Faber as combination warfare, an aggressor can ‘bedevil’ an opponent with ever shifting, multi-dimensional assaults. If applied correctly, this could pose a serious threat to a defender as combination warfare seeks to overwhelm an adversary by assaulting them in as many domains or spheres as possible, seeking to create a sustained, most likely shifting, pressure that is hard to anticipate.

For an actor to apply combination warfare in an effective manner, it is important not to only use the various methods horizontally (i.e. across the columns of the table in figure 1), but also vertically in the following combinations: supra-national, supra-domain, supra-means, and supra-tier (Callard and Faber 63). These combinations can be explained as follows:

***Supra-national combinations***: a combination of national, international and non-state organizations. These blend together and assemble more means to resolve in a range wider than the problem itself. Supra-national combinations are the best way of dealing with contemporary challenges. As stated by Qiao and Wang, the threats to modern nations often no longer come from one or two single countries, but from supra-national powers combining nation states with international “organizations” such as multinationals, religious organizations, NGOs, criminal organizations, etc. (Fridman 15).

***Supra-domain combinations***: military, non-military and above-military forms of warfare. When considering human history, armies merely collided in two-dimensional geographic space at first. Eventually sea and air operations were added, and in contemporary times the domains of space and cyber have also been included.  The authors however pose the questions whether operating in these five domains is “sufficient unto itself”? Certain Chinese strategist for example consider ecological warfare an especially powerful form of war with regards to supra-domain combinations. “Activities in this category could range from burning oil fields to "accidental" chemical spills, to manipulating "natural" meteorological and seismic events (i.e. triggering earthquakes, and altering temperatures, precipitation and sunshine patterns)” (qtd. in Callard and Faber 64). The non-military aspect of supra-domain extend the spectrum of warfare to every field of human activity. By shaping finance, trade, resources, economics, legal means, moral means, and media into forms of warfare, this concept overlaps with Russian chief of the General Staff Gerasimov’s “indirect and asymmetric methods”, referred to above as the ‘Gerasimov Doctrine’. Gerasimov in his 2013 article emphasizes the usage and importance of non-military means to an even greater extent, claiming that war is likely to be conducted for 80% with non-military means and 20% with military measures (Bartles 34). Not only the non-military aspect, but also above-military forms of warfare, including psychological, cultural and diplomatic, as well as technological and R&D warfare, would fit the concept provided by

Gerasimov. These above-military forms are mostly used to assimilate those who have different views through the use of soft (non-coercing) power, negotiation or intimidation (Callard and Faber 64-65).

***Supra-means combinations***: orchestrate all available means, being military, non-military, and above-military to carry out operations.

***Supra-tier combinations***: combining strategic, tactical, and operational levels of a conflict into one campaign.

The concept of combination warfare on both vertical and horizontal levels provides an actor with "a set of cards" being the 27 types of warfare that can be packaged in four supra-level combinations, that in turn can be ordered and picked into a "winning hand". When regarding this combination warfare, anything and everything can be deemed a weapon, which is not only used against enemy combatants but also against the civilian population in a target country. Using the concept of unrestricted warfare as example it can be seen that the notion that war would become civilianised and predominantly non-military as Gerasimov predicted is not new.

## 3.2. New-Generation Warfare

When talking about the concept of hybrid warfare, Russia's actions in Ukraine appear to be a good example. It is framed to be one of the first 'clear' instances were hybrid warfare has been used, according to the *communis opinio* of Western academics, strategists, politicians, and journalists. The Russian Federation, or more specifically its military, is adamant that it does not practice hybrid warfare however, as it sees hybrid warfare as a completely Western concept which in Russia is mostly discussed to mention the West's strategies to weaken Russia. Simultaneously there is a belief in Russia that the concept that hybrid warfare entails, as it is often mentioned by Western analysts, has been practiced since warfare began, and thereby is nothing new, as such deeming the concept mostly useless (Bartles 34). In the article mentioned previously Gerasimov spoke about the changing nature of warfare, using 'foresight' to predict how future warfare would look like. 'His doctrine', can be deemed to be much broader in scope than the Frank Hoffman's original concept of hybrid warfare. An example that can clearly illustrate the difference between the concepts is the Russian understanding of the Colour Revolutions and the Arab spring as forms of hybrid warfare practiced by the West. Additionally according to Gerasimov the influence that NGOs can have on a society can be means of indirect and asymmetric warfare, a notion that does not fit in the Western concept of (hybrid) warfare, at least not in the way Frank Hoffman put it (Bartles 34). According to Gerasimov in 2013 the very rules of war have changed, with a blurring of the lines between peace and war. Non-military means of achieving political and strategic goals have grown, up to the extent that they exceed the effectiveness and power of military means in many cases (Gerasimov 24). While the West often considers non-military measures like economic sanctions, political pressure and suspension of diplomatic ties as ways of avoiding wars, the Russian military staff considers these measures as acts of war (Bartles 34).

So what is the alleged 'Gerasimov Doctrine', often incorrectly referred to as new-generation warfare, exactly? The 'Gerasimov doctrine' is a perceived strategic form and/or method of carrying out combat in line with the concept of hybrid warfare. The concept is based on what Chief of the Russian general staff Gen. Gerasimov described as indirect and asymmetric methods. This concept was introduced a year before the crisis in Ukraine started, and although it overlaps with practices found in Ukraine, Gerasimov was merely explaining his view on the nature of future war, and not proposing a new Russian doctrine (Bartles 31, Galeotti, I'm Sorry for Creating the 'Gerasimov Doctrine). The concept of indirect and asymmetric methods, now incorrectly dubbed new-generation warfare or Gerasimov's doctrine, was based on 'foresight' (explained in chapter 4), a term directly linked to military science in Russian military thought. Within this 'new-generation warfare' the main battlespace is the mind being dominated by informational and psychological operations (Berzins 5). In his article Gerasimov points to lessons to be learned from the Arab spring, explaining that while the events of the Arab spring are not war, in terms of the scale of destruction and casualties, and in the political, social and economic consequences, the outcomes are comparable with any 'real war' (Gerasimov 24).

## 3.3. Gray-Zone Warfare

Newer than hybrid warfare is the concept of the *Gray zone*, and warfare conducted within it. Before continuing on what the concept of the *Gray zone* actually entails, it is important to note that once again there appears to be a great diversity in opinion regarding the matter among academics, similarly to notions regarding hybrid warfare. Some identify Gray Zone conflict as a new phenomenon that will both increasingly characterize and challenge the international system in the foreseeable future. Others however, argue that the concept is overhyped, ahistorical, and in line with critical remarks concerning hybrid warfare, meaningless. An issue that the gray-zone concept faces is shared with many of the previously mentioned terms, being that they appear to encompass a too broad array of behaviours, from irregular to unconventional warfare, from coercion to compellence. Similarly to hybrid warfare, concepts like gray zone warfare cannot encompass everything if they are to be used to describe anything at all.  Enthusiasts of the concepts of gray zone and hybrid warfare often use these concepts to describe the actions of Russia, China and Iran. However, activities of terrorist organizations like Daesh and Boko Haram are also often put under these categories. While both types of examples might not be compatible with the concept of conventional warfare, China's expansionism in the South China Sea and Boko Haram's terrorist activities in Nigeria and neighbouring countries are no way near comparable. This makes it illogical to put both in the same category, as this would cause the definition to become too broad and thereby useless.

Gray-zone conflict is best understood as activity that is coercive and aggressive in nature, although deliberately designed to stay under the threshold of conventional military conflict and open interstate war. Gray-zone conflicts can be regarded as neither war nor peace, but rather lie somewhere in between. One of their most defining characteristics is ambiguity, leaving uncertainty about ultimate objectives, involved actors, whether and which international treaties have been violated, and which response would be appropriate (Bensahel). The goals of gray-zone strategies are to reap gains as associated with victory in war. However, gray-zone approaches are meant to achieve these gains without the conflict escalating to overt warfare, without crossing existing red-lines, and, most importantly, without exposing the practitioner of gray-zone strategies to repercussions and risks that escalation might bring. These approaches are mostly applied by politically revisionist states that are interested in modifying aspects of the contemporary international status quo (Brands 1). In order to prevent the concept of gray-zone warfare from becoming meaningless through including too broad a spectrum of actors, which has been pointed out as an issue mentioned earlier, Brands refers Michael Mazarr's "*Mastering the Gray Zone".* According to Mazarr a defining feature of gray-zone conflict is that it is moderately but not radically revisionist in intent, meaning to say that actors performing gray-zone strategies wish to alter the international arena slightly, but do not wish to destroy it. In addition, he states that it is gradualist and coercive in nature, while being mostly unconventional in the tools it employs (Mazarr 4). Through this definition the activities of Russia, China and Iran can all be deemed of belonging within the gray-zone debate, while the activities of both Daesh and Boko Haram are not to be included, narrowing the scope of the concept of the gray zone and leaving a possibility for the usefulness of the concept.

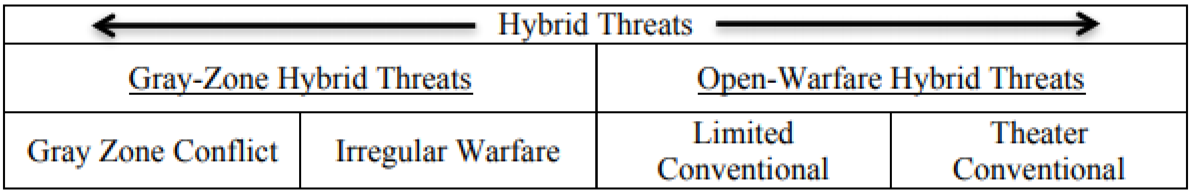
When following Brands definition on what gray-zone conflicts entail, it can be determined that the most attractive gray-zone strategies are those that avoid activities that are recognizable on the conflict spectrum, in order to prevent an actual conventional war. The best possible outcome for gray-zone strategies would be to achieve the set goals without the adversary realizing that a conflict is taking place, thus preventing escalation. These kinds of strategies are obviously not without risk, since a chance exists that a target may retaliate once it realizes what is happening. However, a target that wishes to openly retaliate likely suffers higher costs since “the target state would have to undo the fait accompli and change the new status quo” (Bensahel). In addition, it might be difficult to gain public support, especially in democratic countries, when one wishes to retaliate militarily.

A conceptual weakness of gray-zone conflicts is that there often appears to be a lack of terms and policies for when a conflict stops being a conflict or is not defined as conflict through the usual definitions, as for example the one provided by the Uppsala Conflict Data Program. While victory in conflict or war could previously only be achieved through the use of military force, the increase in which daily life in both economic and social ways is dominated by the internet and various other information technologies has created new challenges. The notion of unrestricted warfare, a concept written about by the two Chinese Colonels in 1999 mentioned earlier, is less farfetched in 2018 than it was in 1999 (Liang & Xingsui). Whereas geography plays an important role in conventional wars, whether it being land, sea or air warfare, the interconnected world of the 21st century allows for adversaries behind keyboards, rendering geography and the support of a strong nation state irrelevant, as a single individual can already strike at nearly every facet of a society without ever using or encountering military force. Bensahel states that although conventional military force can still be deemed of importance, one should note that many conceptions of conflict and warfare are less relevant in the present, as gray-zone conflicts and unrestricted warfare are no longer limited to being predominantly of military nature. Instead strategies have developed to the point where a distinction between war and peace may become unclear, and these distinctions might not be meaningful anymore at all (Bensahel).

To further complicate things, John Chambers continues on the concept of the gray zone by combining it with hybrid warfare, which does lead to more labelling and typology, but simultaneously narrows the topics down in a pragmatic and usable way. According to Chambers, the gray zone is the space between peace and war, breaking the binary aspect of the two: “it is an operational environment churning with political, economic and security competitions that require constant attention” as Chambers quotes Schadlow (Chambers 4; Schadlow). Moreover, gray-zone conflicts can be a form of hybrid threats, but hybrid threats are not confined to the gray zone. Instead Chambers splits hybrid threats into two categories: gray-zone hybrid threats and open-warfare hybrid threats, which can be further divided (Figure 2). He states that open-warfare hybrid threats can be compared to hybrid warfare as described by Frank Hoffman, and are of military nature. Gray-zone hybrid threats, however, contrary to Frank Hoffman’s concept, rely more on ambiguity, exploiting an adversary’s weakness through DIME (soft power: Diplomatic, Information, Military, Economic; Hillson 235), and non-attribution (Chambers 5). Chambers points out that for the

United States new-generation warfare conducted by the Russian Federation, is an important example of gray-zone hybrid threats, which takes advantage of the United States government's bureaucracy. It targets "Phase 0" of United States military operations (also called the "shape" phase), which is defined as "Joint and multinational operations—inclusive of normal routine military activities—and various interagency activities [. . .] performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies" (Chambers 6). This is the phase in which United States doctrine addresses what can be considered gray-zone conflict. During this phase the Department of Defense often is not the lead operating agency as it would be during conventional conflict (see Figure 3).

*Figure 2. Hybrid threats according to John Chambers*

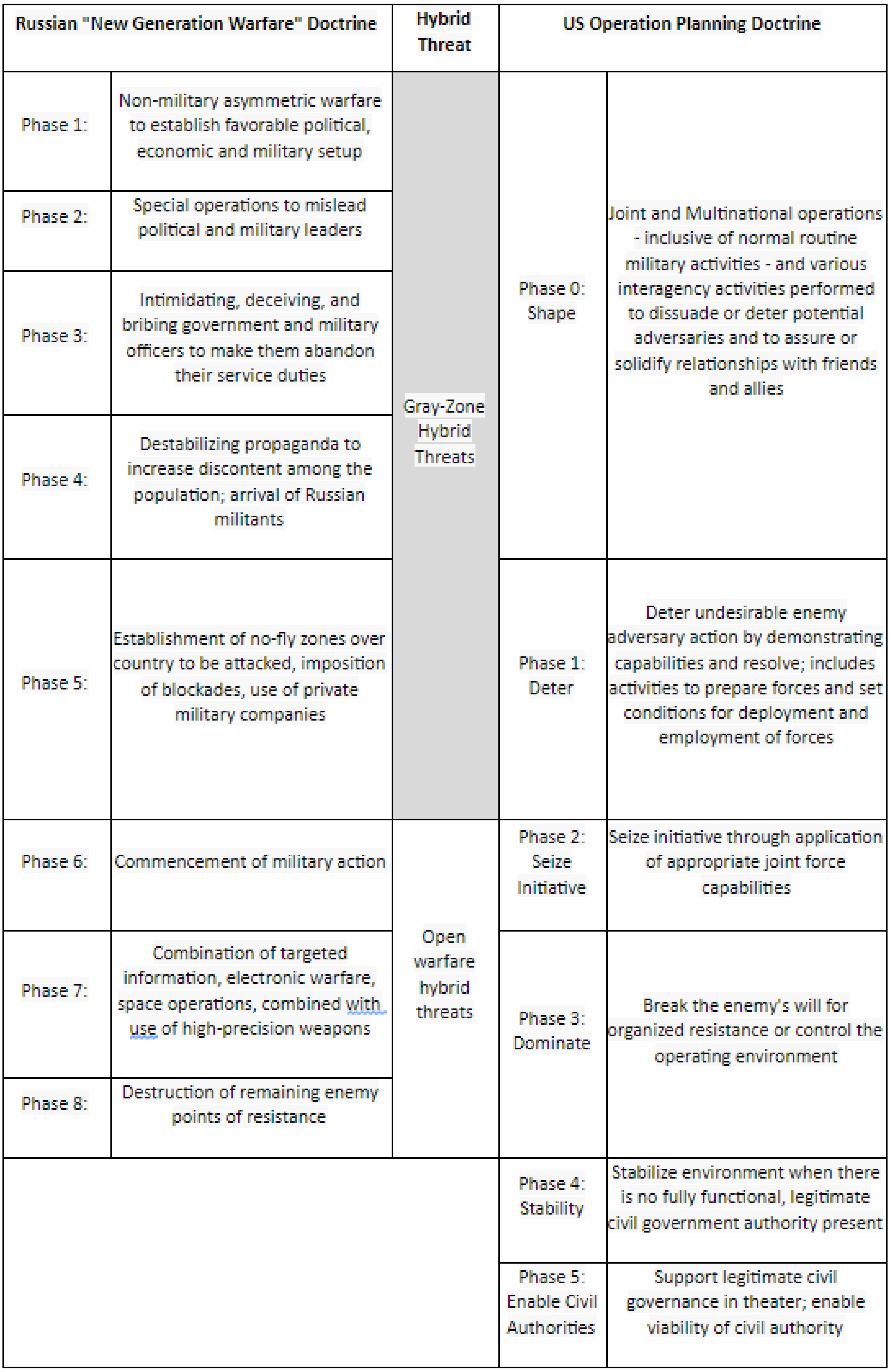


| ← Hybrid Threats → | | | |
|---|---|---|---|
| Gray-Zone Hybrid Threats | | Open-Warfare Hybrid Threats | |
| Gray Zone Conflict | Irregular Warfare | Limited Conventional | Theater Conventional |

*Source: Chambers 5*

As seen, the gray zone and gray-zone conflicts have a variety of definitions. They can be characterized by "intense political, economic, information, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war" (Votel 101), or described as a space between peace and war, boiling with political, economic and security competitions that require constant attention (Schadlow). Chambers considers the gray zone to be an operational environment, similar to how urban or desert warfare both refer to operational environments in which the conflict takes place. As such he does not consider it a distinct type of conflict (Chambers 13).

*Figure 3. Comparison of Russia's and US Doctrines on "Hybrid Warfare"*



| Russian "New Generation Warfare" Doctrine | | Hybrid Threat | US Operation Planning Doctrine | |
|---|---|---|---|---|
| Phase 1: | Non-military asymmetric warfare to establish favorable political, economic and military setup | Gray-Zone Hybrid Threats | Phase 0: Shape | Joint and Multinational operations - inclusive of normal routine military activities - and various interagency activities performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies |
| Phase 2: | Special operations to mislead political and military leaders | | | |
| Phase 3: | Intimidating, deceiving, and bribing government and military officers to make them abandon their service duties | | | |
| Phase 4: | Destabilizing propaganda to increase discontent among the population; arrival of Russian militants | | | |
| Phase 5: | Establishment of no-fly zones over country to be attacked, imposition of blockades, use of private military companies | | Phase 1: Deter | Deter undesirable enemy adversary action by demonstrating capabilities and resolve; includes activities to prepare forces and set conditions for deployment and employment of forces |
| Phase 6: | Commencement of military action | Open warfare hybrid threats | Phase 2: Seize Initiative | Seize initiative through application of appropriate joint force capabilities |
| Phase 7: | Combination of targeted information, electronic warfare, space operations, combined with use of high-precision weapons | | Phase 3: Dominate | Break the enemy's will for organized resistance or control the operating environment |
| Phase 8: | Destruction of remaining enemy points of resistance | | | |
| | | | Phase 4: Stability | Stabilize environment when there is no fully functional, legitimate civil government authority present |
| | | | Phase 5: Enable Civil Authorities | Support legitimate civil governance in theater; enable viability of civil authority |

*Source: Adapted from Chambers 3*

## 3.4. Summary of this Chapter

We can sum up the (mostly Western) writings presented above concluding that:

Firstly: Hybrid warfare, gray-zone warfare, and all terms that fit in between, are arguably not new concepts. They do however provide new challenges mostly due to the rise of globalisation and interconnectedness. The new technologies employed, especially in the cyber domain, challenge current concepts of war and peace.

Secondly: Although occasionally criticized by various academics, the concepts of hybrid warfare, gray-zone warfare, new-generation warfare, and the so-called 'Gerasimov doctrine' are used to label and explain Russian actions since the annexation of Crimea in 2014. A variety of issues with these concepts exist however. A consensus about the meaning of either of these concepts, but especially about hybrid warfare, appears to be absent. Nonetheless hybrid warfare has become iconic for how 'the West' perceives Russian threats, witnessed by the fact that not only the media, but also policy papers, intelligence agencies and many publishing military officers have adopted the term 'Russian hybrid warfare'. Depending on what is meant by hybrid warfare, it often remains vague whether non-kinetic elements are included. Hybrid warfare along the lines of Frank Hoffman's original definition lacks non-military methods and effects, is limited to the tactical or operational level, and includes both state and non-state actors. Newer term(s) however, often associated with Russia's recent actions, have expanded to fit a strategic level, taking into account non-military methods, but are limited to state-actors. As such the applicability and usefulness of the term depends on which sort of hybrid warfare is meant. The fact that this distinction between definitions of hybrid warfare can be made, arguably leads to confusion rather than to a clarifying and usable concept.

Thirdly: Much, but not all, of Western writing about Russian hybrid warfare fails to take into account Russia's perspective, and instead views it through a 'Western lens'. One example of this is the reference to the 'Gerasimov doctrine' from 2013, which was not meant to be a doctrine. Instead it attempted to provide an explanation of how Russia regarded recent uprisings such as the Colour Revolutions and Arab Spring, considering these to be forced regime-changes and a form of warfare it would need to prepare against. Contrary to Russian opinion, these events do not fit in the Western concepts of war or warfare. Utilizing Western terms and concepts to define a Russian approach to warfare, or even a greater Russian strategy, is likely inaccurate. This was well-phrased by Timothy Thomas, with whom we conclude: 'Simply overlapping Western concepts on Russian thinking doesn't always work. If evolving foreign concepts are not understood from their local context, then the West will always be chasing after outliers without understanding where they fit in Russia's overall theoretical and planning process.'" (Thomas 574).

# 4. Russian Opinion and Usage of Hybrid Warfare

Although hybrid warfare is often used to describe Russia's actions in Ukraine since 2014, Russia itself has a different opinion and theory on what hybrid war entails. The Russian literature uses the term *Gibridnaya Voyna* (Гибридная Война), which is a literal translation of hybrid warfare.

One of the biggest issues with the usage of the term hybrid warfare, is that the (Western) international community has almost universally accepted the term to refer to Russia's recent actions in Ukraine, and expect Russia to continue on this path with hybrid warfare as its main choice of tactics and/or strategy (Hunter & Pernik 3). Russian academics and military staff themselves, however, have a very different opinion on *Gibridnaya Voyna*, and in addition make a distinction between this and new-generation warfare. This chapter will sum up the Russian view and practice regarding *Gibridnaya Voyna* and will explain the differences between Russian and Western conceptualizations.

## 4.1. Russia's Usage of Hybrid Warfare

Although Russia has a different opinion on what *Gibridnaya Voyna* entails, its annexation of Crimea, its political and military support of pro-Russian separatists in eastern Ukraine, and also its hacking of the DNC (Democratic National Committee) are often used as prime examples of hybrid warfare. It has been observed that Russia uses multiple instruments of power and influence to pursue its national interests outside of its own borders, often at the expense of the United States of America or its allies (Chivvis 1). Since Russia recognizes that it stands little chance in a (protracted) conventional conflict against NATO, Moscow seeks to pursue its interests without overt usage of its military power. Although Russia is prepared to use conventional or even nuclear threats as part of a (hybrid) strategy, it is seen to prefer to minimize its use of conventional force. Cyber tools are often employed to achieve goals without overt military presence, something that Chivvis describes as economizing the use of force. Allegedly Russia's operations break down the binary delineation between war and peace, which follows the definition of gray-zone operations, and is ever-changing in its intensity. Moreover, the actions are described as population-centric (emphasising the importance to influence the population), which is something that Russian military experts have learned from wars fought by the United States and its allies in the Balkans and Middle East the past 25 years. According to Chivvis: "They seized upon the importance of an approach that seeks to influence the population of target countries through information operations, proxy groups, and other influence operations. Russia uses hybrid warfare to work within existing political and social frameworks to further Russian objectives." (2).

Philip Karber has a different view on Russia's threats for the west. Instead of joining in Western views on hybrid warfare, he points to new-generation warfare which targets Western weaknesses and combines low-end hidden state involvement with high-end superpower involvement. He states the approach consists of five elements: political subversion, proxy sanctuary, intervention, coercive deterrence, and negotiated manipulation, as can be inferred from Russia's actions in Ukraine. Although Gerasimov is often credited for Russia's 'new-generation warfare', the concepts of Karber and Gerasimov do not neatly correspond, since Gerasimov's aim was to predict what future warfare would look like, while Karber shares his opinion on how current Russian military doctrine works. In addition, it was not Gerasimov who came up with new-generation warfare, but Colonel Chekinov and Lieutenant General Bogdanov, as will be explained below. According to Karber, Russian new-generation warfare can be described in five stages:

***1. Political Subversion***: This stage consists of both insertion of agents on the ground and of information operations, mainly using modern mass media to exploit ethnic, linguistic, and class differences. It spreads news about corruption, while compromising and intimidating local officials, which is backed up with kidnapping, assassinations and terroristic acts. Simultaneously discontented elements in the target country are recruited.

***2. Proxy Sanctuary***: During this step local governmental centres, police stations, airports, and military bases are seized, while insurgents are armed and trained. The setting up of checkpoints, denying usage of infrastructure, combined with cyberattacks and a referendum wherein only a single party is represented is used to establish a pro-Russian (or Russian influenced, if not controlled) "People's Republic".

***3. Intervention***: Thirdly Russian forces are deployed in sudden large-scale exercises along the border of a target country while simultaneously providing insurgents with heavy weapons (tanks, artillery, anti-aircraft machinery). Additionally training camps along the border are, where insurgents and "volunteer" battalions can be trained, the latter of which are to be integrated as proxy troops.

***4. Coercive Deterrence:*** The fourth stage continues on the third stage with the forward deployment of tactical nuclear delivery systems combined with aggressive air patrolling of the neighbouring areas to prevent involvement from the target or other actors.

***5. Negotiated Manipulation***: The final stage is meant to use (or abuse) Western negotiated ceasefires. These ceasefires can be (ab)used to rearm proxies in the target area and they can be violated to bleed the adversaries forces (as was seen in Ukraine). Simultaneously other states are discouraged to help the adversary because of the fear of escalation, while attempts are made to divide the Western alliance by the use of economic incentives, and selective negotiations.

When comparing Karber's five stages to Gerasimov's attributed Doctrine, a major distinction can be made. Whereas Gerasimov emphasized the importance and application of non-military means, Karber's stages rely mostly on military means and only have a few non-military aspects. While this is partially in line with Chekinov and Bogdanov's new-generation warfare, as will be shown in the next section, various of Karber's stages can be deemed case specific or circumstantial, as they rely on connected borders and a weaker adversary. Military exercises as deterrent, supplying heavy weapons, and creating training camps, as described in the intervention stage can still be done without shared borders, but are less likely to be successful and harder to apply. Another issue with Karber's interpretation of new-generation warfare is that it appears to focus on usage against a weaker opponent, and would be less of a threat against a country of similar power or greater power, let alone NATO after invoking article nr. 5.

As Figure 3 in chapter 3 shows Chambers summed up Russian new-generation warfare more elaborately than Karber. As shown there are quite some differences between the operational phases of the Russian Federation and the United States of America. Not only is there a difference in the number of phases, but also when these phases occur, and what the actions in these phases entail (Chambers 26). As Major John R. Davis Jr. argues that Russia has combined various military forms of warfare with economic, information and diplomatic instruments of power into a hybrid threat whole of government approach (23). In order to keep a conflict below the threshold normally deemed necessary for invoking NATO's Article 5 Collective Defence Guarantee, Russia is employing its hybrid threat approach during Phase 0 (Shape) of Joint and Multinational Operations as can be seen in figure 3 (Davis Jr. 23, Weitz).

## 4.2. Russian Opinion on Hybrid Warfare

One recurring term when analysing "Russian hybrid warfare" is the alleged Gerasimov Doctrine, which is not a doctrine at all. Although often interpreted otherwise General Gerasimov did not mean to propose a 'new' Russian way of warfare or a new military doctrine. As explained by Bartles, Gerasimov's article is used to provide a prediction about the future of warfare. The Russian general staff is expected to use 'foresight' to develop theory and practice of future war, which is the context in which Gerasimov's article is written. The term "foresight" even has a specific military definition in the Russian lexicon: "Foresight (military) is the process of cognition regarding possible changes in military affairs, the determination of the perspectives of its future development. The basis of the science of foresight is knowledge of the objective laws of war, the dialectical-materialist analysis of events transpiring in a given concrete-historical context" (qtd. in Bartles 31). The concept links foresight directly to military science, with military science being the science of future war.

Meanwhile, Mark Galeotti, who coined Gerasimov's prediction about future and contemporary warfare the 'Gerasimov doctrine', has apologized for the confusion he unintentionally created. Galeotti says: "So for a snappy title, I coined the term "Gerasimov doctrine," though even then I noted in the text that this term was nothing more than "a placeholder," and "it certainly isn't a doctrine." (Galeotti, *I'm Sorry for Creating the 'Gerasimov Doctrine'*). The idea of the 'doctrine', instead of proposing a new formula for Russia's armed forces to act in future wars, was to explain how Russia was seeing recent uprisings such as the "Colour Revolutions", the Arab spring, and (shortly after Gerasimov's article was published) the Maidan revolution. The often-recurring misunderstanding of Gerasimov's intentions show a limited understanding of Russian military ideas, which are often regarded through a Western conceptual lens.

### 4.2.1. Hybrid Warfare, Gibridnaya Voyna and New-Generation Warfare

Similarly to Western academic and professional circles, there are multiple approaches to what *gibridnaya voyna* entails. The most prominent Russian narratives on hybrid warfare only share the name (albeit translated) with the West, as nearly all ideas regarding this concept appear to differ from the western concept (Fridman 92, Galeotti, *I'm Sorry for Creating the 'Gerasimov Doctrine'*). Hybrid warfare, as in its original form described by Frank Hoffman, focuses on the hybridization between different military means and technologies on operational and tactical levels. Adaptations of the concept after Russia's actions in Ukraine provide a similar focus, but in addition also encompass political, social and economic actions without boundaries between covert and overt actions.

*Gibridnaya voyna* differs from the aforementioned concepts in that it is not considered to be a war at all, despite having the word '*voyna*' (a translation of 'war') in its name. The Russian concept of "new-generation warfare" is more in line with recent Western interpretations of hybrid warfare. Whereas hybrid warfare and new-generation warfare, among other terms, are often used interchangeably when describing Russian military activities or doctrine in Western circles, Russia actually considers these do have different meanings. Russian colonels Chekinov and Bogdanov made a distinction between new-generation warfare and *Gibridnaya voyna* in their article 'The Nature and the Content of the New-Generation War'. (Chekinov & Bogdanov). This article is less referenced than Gerasimov and is also often misinterpreted among most Western experts. Chekinov and Bogdanov claim that new-generation warfare uses non-military means as a preparation for military actions and falls in the category of war, while *gibridnaya voyna* sticks to non-military means that are not meant to introduce military action, therefore not fitting the category of war. Experience gained from the last decade shows that the intensity of conflict in spheres other than that of armed struggle has significantly increased, whereby goals can be achieved with non-violent means, and without the use of military force. Chekinov and Bogdanov argue that, in line with this experience, *gibridnaya voyna* can be defined as political conflict or competition in inter-state confrontations, which is intended to realise national interest with the use of indirect actions, and whereby the military is only used as a deterrent in the background (qtd. in Fridman 132, 136).

Overlapping with *gibridnaya voyna,* new-generation war also employs non-military methods, especially information- and psychological operations as integral parts. These actions mainly take place during a preparatory stage before a war. In contrast to *gibridnaya voyna*, new-generation war is seen as an international armed conflict. Non-military actions, which can include, but are not limited to informational, diplomatic, economic, and psychological confrontations, are used to create favourable conditions for the deployment of armed forces (Fridman 131). Chekinov and Bogdanov explain Russian military expectations for future full-scale wars along the lines of new-generation warfare. They depict war to start with information- and psychological operations alongside cyberattacks, followed up by a 'shock and awe' offensive with massive airstrikes, after which a phase of land combat follows with all its conventional instruments, such as tanks, artillery and soldiers. As Galeotti states:  This is a far cry from the imagined semi-covert, spooks-and-trolls 'hybrid wars' often imagined in the West, which are best considered 'political wars' (Galeotti, *i'm Sorry for Creating the 'Gerasimov Doctrine'*).

#### 4.2.2. Gerasimov Doctrine 2.0

Almost six years after the Gerasimov ideas were coined a doctrine by Galeotti, on the 2nd March 2019, General Gerasimov did present a new report, which demonstrates a clear difference between how the West sees future Russian conflicts from how Russia itself envisions them. Gerasimov's tone has grown in hostility when compared to his original 2013 article (which was published in English in 2016), with the United States and its allies openly named "aggressors" and "probable enemies". Gerasimov now says that Russia has to prepare to fight different types of battles using military and non-military (information warfare) means (Felgenhauer). According to Gerasimov the Pentagon is developing a new aggressive strategy nicknamed "Trojan Horse", which focuses on the "protest potential of a fifth column" combining colour-revolution with the use of high-precision weaponry against important targets, with as purpose to undermine and overthrow foreign governments, referencing to Iraq, Libya and Ukraine (McDermott). While Gerasimov points out the importance of non-military means, he declares that: "The main substance of [Russia's] military strategy is preparation for war using primarily the Armed Forces". And while non-military means might aid in achieving military goals, the military may coordinate them, but should not lead them (Felgenhauer). For the military the focus should be on "active defence", which can be achieved by pre-emptively neutralizing threats. In order to do so, Gerasimov stresses the need to upgrade both non-nuclear and nuclear strike systems, modern weapons, digital technologies, unmanned systems, and electronic warfare capabilities (Felgenhauer, McDermott). Comparing this to the previous perceived 'Gerasimov Doctrine' it can be seen that the emphasis on military means has grown, and is more in line with what Chekinov and Bogdanov wrote about new-generation warfare.

## 4.3. Summary of this Chapter

The conclusion that can be drawn on the basis of this chapter is that at least three completely different phenomena have been described as Hybrid War.

Hoffman's original focus on the tactical and operational levels represents the first conceptualization. He incorporated different modes of war, such as conventional capabilities, irregular tactics, terrorist acts and criminal activity.  His notion was not intended as a grand strategic plan for the army in the long run. Still, most of the criticism that the concept attracted was that it was not sufficient strategically. Secondly, after Russia's actions in Ukraine, the concept got new life, and was broadened with diplomatic, political, economic, and social actions, bridging the gap between hard and soft power. Thirdly, Russia's concept of Hybrid Warfare (*gibridnaya voyna*) was discussed. Russia's concept differs greatly from both Hoffman's hybrid warfare, (and from the definitions by NATO and many Western academics), in the sense that it minimizes military action, and focuses mostly on information and psychological pressure, being more comparable with information- or political warfare), without considering *gibridnaya voyna* as actual war. Contrary to *gibridnaya voyna,* a concept referred to as 'new-generation war' appears to be more similar to Western concepts of hybrid war, which, although it relies on the incorporation of non-military means, is considered to be actual warfare.

When taking the Ukraine crisis as an example, all concepts of hybrid warfare can be applied to some degree. Pro-Russian separatists use both conventional and irregular tactics, technologies and methods of warfare against the Ukrainian army, which can be called hybrid warfare in the sense of Hoffman's definition. Russia's use of covert and overt military and non-military means and methods against Ukraine fits NATO's definition of hybrid warfare. And the West's use of non-military subversive means and methods against Russian geopolitical interests, as a continuation of the NATO strategy against the USSR, does fit Russia's definition of *Gibridnaya Voyna*.

Since the term hybrid warfare can apply to all that is mentioned above, covering a wide variety of methods and means, it has mostly been rejected by military organizations worldwide, who are more in favour of case-specific definitions. However, the quick and successful politicisation of the term does not come as a surprise, as nearly every perceived hostile act can be placed in the same conceptual framework, thereby establishing a continuity in political narrative, which allows different domestic actors to close ranks against an external threat (Fridman 157). This politicisation is however conceptually dangerous, as it is not in line with Russia's most recent conceptualizations of contemporary warfare. While non-military means are deemed to be important, they should not be overemphasised according to the Russian military and its General Staff. Contrary to the idea of Russian hybrid warfare, General Gerasimov and Colonels Bogdanov and Chekinov emphasise the importance of a strong and modern military power to win future conflicts. In these expected future conflicts non-military means such as information and psychological operations merely serve as support, whereas the conventional army is deemed to be decisive.

# 5. The Politicisation of Hybrid Warfare

## 5.1. Academic versus Political use of Terms

As mentioned previously, there are multiple terms that are similar to hybrid warfare currently in use. to describe Russia's actions since its annexation of Crimea. Whether these terms are agreed upon by researching specialists or not tends to be overlooked. The terms have been politicised, and even although some might be too broad to be academically meaningful, they are still used politically or pragmatically for explaining current threats. Especially Hybrid warfare, has become a synonym for Russia's broad range of subversive instruments, most of which are of non-military nature as Christopher Chivvis of the Rand corporation states in his testimony for the Committee of Armed Services and the United States House of Representatives. The Dutch Military Intelligence and Security Agency (MIVD) also uses the term of hybrid warfare when describing both Russian actions and threats over the past years, with the term hybrid warfare recurring in their annual reports of 2016, 2017, and 2018 (Ministerie van Defensie). Chivvis' testimony and the annual MIVD reports vary in the description of Russian actions and threats, especially where the annual reports take a broad range of Russia's tools as an actor into account, whereas the RAND testimony focuses on specific hybrid threats. However, both MIVD and RAND emphasize cyber and information operations as an important aspect of contemporary hybrid threats.

Politicisation has had a huge impact on the theory of hybrid warfare. Many differences between hybrid warfare as coined by Frank Hoffman, and contemporary use of the term hybrid warfare can be found. Whereas Hoffman's theory was limited to the tactical and operational (military) levels of a conflict, more recent conceptualizations have expanded it to fit the strategic level. A conceptual transformation of the theory has taken place, broadening beyond its former definition. After analysing Russian actions in Ukraine, the International Institute for Strategic Studies (IISS) labelled hybrid warfare: "the use of military and non-military tools in an integrated campaign designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilising diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure" (Fridman 106). Where the concept of hybrid warfare originally was limited to the military realm, it has evolved to include non-military means as well.

## 5.2. Framing Russia as a "Hybrid Aggressor"

In 2015 more than half of NATO's Defence College (NDC) publications discussed a topic called 'Russian Hybrid Warfare' (Fridman 106). Although there has been a lot of criticism on the concept of hybrid warfare, it pales into insignificance when compared to the amount of literature that claims Russia is simply using it. It seems that whether such a statement is true or not is not too relevant, as the frequency of use appears to shape the truth.

It can be disputed in how far the concepts of hybrid warfare, gray-zone conflicts, new generation warfare, or combinations of the former as seen by Chambers (e.g.: gray-zone hybrid threats), are something new. More important than the novelty of these concepts is the relevance of the actions they try to describe and define. Whether we are dealing with old wine in new casks or not, we need at least clarity (if not consensus) regarding the usage of these terms. Currently however, many policymakers, journalists, academics, and defence staff use these terms rather indiscriminately or loosely to describe recent actions, mostly by Russia, but also by China and Iran to point to issues that are currently unsolved. As Patrick Duggan, who considers hybrid warfare to be nothing new, but merely a "hodgepodge" of conflicts fused together by technology, states: "These 'hybrid-threats' confound establishment-thinking seemingly more preoccupied with conflict typology, than the innovation of new organizational concepts to counter them. Success in warfare is not derived by labelling its assembled parts, it is achieved by correctly assembling emerging technology and new capabilities into trusted fields of practice" (Chambers 6). Whether the name fits is not the most important question. Instead one should focus on what to do with the perceived hybrid threats, as their recent emergence in discussions concerning conflict, whether it be among policymakers, scholars, or strategists, highlights importance.

The politicisation of hybrid warfare has not prevented further critique on the concept of (Russian) hybrid warfare. In the implementation of the Government Plan for Analysis, Assessment and Research for 2016, published by the Prime Minister's Office of Finland, Bettina Renz and Hanna Smith argued that the concept of hybrid warfare does not adequately reflect Russian military modernization, as it understates Russian ambitions while overestimating Russian capabilities simultaneously. Too often it is described as a new war-winning formula, not taking into account that Russian actions in Ukraine were case specific and cannot be reproduced without a similar context existing. In addition, the broadness of the concept of hybrid warfare oversimplifies Russia's foreign policy and does not provide useful goals or intentions (p.8/9). Instead of clarifying Russia's stance within international politics, the notion of Russian hybrid warfare obscures it and blurs the lines between peace and war, thus increasing the difficulty of identifying realistic policies against Russia, while militarizing the West's language regarding relations with Russia in the tensest situation since the dissolution of the Soviet Union.

When looking at the military side of Russian operations in Ukraine it can be seen that many of the tactics used were mostly based on traditional Russian or Soviet warfare refitted for modern war. Innovation was not the most notable in the military tactics employed, but in the seamless transition from peace to war (Bruusgaard 81). Moreover, the West was not properly prepared for Russia's appliance of cyber or information warfare. "Crimea demonstrated that Russia does not have to wait until its military transformation is complete to use military force successfully. This is due to two key force multipliers: first, Russia's political will to resort to force when necessary, entirely absent in Europe; and second, the successful integration of other strategic tools such as information warfare, reflecting the new doctrinal emphasis on influence rather than destruction." (Giles 48).

This emphasis on influence, undermining an adversary's legitimacy instead of destroying it, is one of the main reasons why Russian information & cyber warfare should be looked at separately, instead of as part of an overarching hybrid warfare method (Giles 46; Fridman118). This is especially true, because it is often unclear when cyber or information warfare can be seen as actual acts of war, more so when they are not causing kinetic effects. Basic terminological agreement, strategy, and national and international information sharing regarding cyber threats, as well as a consensus about when a network intrusion (hacking) and digital sabotage become acts of war, appear to be absent (Hunter & Pernik 3). Additionally, there is a difference between the Western concept of "cyberspace", and the Russian more comprehensive "information space". In the Russian interpretation, both digital-technological and cognitive-psychological operations are included in information warfare, whereas in the Western interpretation cyber warfare and information warfare are seen separately (Kukkola et al. 28).

## 5.3. Summary of this Chapter

In the West, the politicisation of the concept of (Russian) hybrid warfare can achieve unity against a single opponent, and a continuity in a narrative of constant besiegement, if every action performed by Russia can be called warfare. It provides politicians with the ability to blame Russia (or any other country using this broad array of actions) for every negative occurrence in a country. While this can be useful for politics on a national level, it might be dangerous on an international level. As Russian actions are often watched through a Western lens, its goals or intentions are not taken into account, its future strategies are likely misjudged, and realistic policies regarding Russia become harder to shape. Additionally, the politicization of hybrid warfare brings with it increasingly militarized narratives reminding of the Cold War.

# 6. Cyber Warfare

## 6.1. Introducing the 5th Domain: Cyberspace

Both conflict and war, whether it is a hybrid, of a new generation, or taking place in the gray zone or not, has a relatively new (5th) domain: cyberspace. A domain which influences the evolving character of conflict which is currently being faced, and appears to lead to convergence. The phenomenon that is often referred to as hybrid warfare seems to surge as a result of tightening interaction between humans, the physical world, and cyberspace. These connections, a merging between man and machine into a "cybered world", produce new class of threats. Due to the increasing affordability and sophistication of technology, every country, non-state actor, or even empowered individual, can use hybrid tactics or threats as a useful means to inflict disproportionate harm against an opponent, relative to the size, resources, or geography of the adversary (Duggan). The Russia-Ukraine conflict sheds light on the new technological character of war. Currently (American) policymakers appear to be unable to articulate actionable desired effects, and to deter gray-zone type incursions, due to a lack of understanding of non-kinetics and cyber operations (DeWees et al. 20).

Not only cyberspace influences the evolution of warfare. The shift from sword to rifle, from horse to tank, the addition of warships, airplanes, missiles and drones, all made changes to how wars are fought. These technological improvements are all used to cause kinetic effects, whereas the information domain includes an important non-kinetic element to warfare. Information warfare, hacking, disrupting communication, and spreading misinformation among other things, and the way they are implemented, are increasingly of importance.

Technological progress alone will not automatically lead to victory, as can be derived from the example of the predecessor of digital communication, the telegraph. Duggan states that the first comparable rapid technological progress originated from the Crimean War (1853-1856), referring to the usage of the telegraph (Duggan). When the telegraph was first used in combat, it was not utilized by the military up to its full potential. It was labour intensive, problematic, and commanders had poorly prepared for its tactical benefit. Moreover, the telegraph was used by war correspondents to provide the 'home front' with information about the battlefield on a daily basis, which increased the issues military commanders had with politicians and the public opinion in their country of origin. Therefore, it may come as no surprise that the usage of the telegraph during the Crimean war is mostly remembered as a tool in which the front became connected to European audiences in their home countries, with bureaucrats and politicians micromanaging their armies, providing them with questions, suggestions, and orders from afar; best described as armchair warriors interfering with the battlefield from back home.

As Duggan quotes: “A key lesson as history moves forward, is that ‘those militaries that took best advantage of the new technologies of the industrial age were not those that acquired the machines or weapons first, but those that recognized the broader informational implications and strove to organize themselves accordingly.’” (qtd. in Duggan73).

When regarding the various domains in which war can take place, a big distinction can be made between the newest (fifth) addition and its four predecessors. The first four domains in which warfare took place, one by one are all of physical, tangible, nature. Within the domains of land, sea, air and space the effects of military action are mostly measured in terms of physical outcomes. This has provided a focus on the “linear measurement” of death and destruction caused by kinetic instruments of power and war. This emphasis on the physical domains often causes a neglect for important characteristics of warfare such as motivation, will, patriotism, etc., best encompassed by the term “moral forces”, as how Clausewitz describes them (Clausewitz 108-109). DeWees et al. justly state that the physical outcomes of kinetic operations are measurable with a certain degree of precision. The moral effects of these operations are however much harder to measure, because they require a form of “military empathy”, being the ability to consider the adversary’s perspective. With the addition of a new, far less physical domain such as cyber, which has substantial non-kinetic as well as kinetic potential, it becomes even more challenging to consider the adversary’s perspective (DeWees et al. 17). In order to better understand the effects of war, DeWees et al. have come up with what they call “the arc of effects” ranging from physical to moral effects.

Realizing the challenges provided by the relatively new cyber domain is difficult without proper experience within the domain. A good example about a similar lack in experience in another domain (sea) can be distinguished during the First World War. Shortly before the First World War broke out, a fictional account written by Sir Arthur Conan Doyle described how Great Britain could be isolated and defeated by unrestricted submarine warfare. This was a concept which did not fit in with the naval zeitgeist. The concept took place in a new domain of warfare, below the surface of the sea instead of on the waves. Traditional forces were slow to understand the importance of the difference, leading to ignorance concerning its potential impact. As soon as submarine warfare took shape, countries were quick to realize the physical results in terms of losses of this new form of warfare, however they were less quick in recognizing its potential effects on the morale through fear on the moral side of the spectrum (DeWees et al. 17). A similar form of fear can be encountered in Ukraine, where Russia employs unmanned aerial vehicles (UAV) for intelligence, surveillance, reconnaissance and target acquisition for artillery. As Ukrainians have observed up to eight Russian UAV overflights on a daily basis, the constant awareness of being observed and possibly targeted instils fear and limits movement. (Karber)

The new domain of cyber within the security environment can be compared to the story presented above. Due to the existing emphasis on physical outcomes, and thereby the physical end of the arc of effects, many fail to fully define and understand the extent of the (mostly non-kinetic) effects provided by the relatively new cyber domain. This lack of understanding limits the capacity for devising an effective deterrent along the full range of security threats, and provides an adversary with relatively greater freedom of movement.

## 6.2. Cyberspace and/or Information Domain

Similar to the broader concept of hybrid warfare, a challenge with regards to cyberwarfare and information warfare once again lies in their conceptualisation. Western policymakers and military strategists appear to make many uninformed assumptions regarding intentions and risks based on their own conceptualisations of “cyber” (Connell & Vogler 1). While the West makes a distinction (albeit partially overlapping) between cyberwarfare and information warfare, Russia does not. Cyberwarfare, similarly to hybrid warfare, is generally only used by Russia when referring to the West. Instead of using cyberwarfare, Russian military theorists use the word informatization, thereby placing cyber operations within the broader concept of information warfare. This does not only encompass computer network operations, but also electronic warfare, (dis)information operations, psychological operations and political subversion, giving the state the means to dominate the information landscape (Connell & Vogler 2-3, Kukkola et al. 28). Therefore, information warfare is a better term when describing Russian cyberoperations.

One of the most important components of the cyber domain is the Internet of Things (IoT). This encompasses everything that is connected to the internet including phones, computers, smart-televisions, means of transport, security cameras, air control systems, power plants, thermostats, refrigerators, and so on. The Internet of Things can be attacked in both kinetic and non-kinetic ways, and attacking information systems is part of information warfare. Kinetic activities within this domain have the goal to damage a certain target, as witnessed both in the first Gulf War and the 2008 invasion of Georgia. There it was used to attack *Command and Control (C2)* systems, thereby disabling governmental, military and logistical communications systems (Hunter & Pernik 5). Its activities and challenges are not limited to kinetic activities however. As Gery et al. cite Brian Nichiporuk, the author of *U.S. Military Opportunities*: “The goals of an offensive information-warfare campaign are to deny, corrupt, degrade, or destroy the enemy’s sources of information on the battlefield. Doing so successfully, while maintaining the operational security of your own information sources, is the key to achieving “information superiority”— that is, the ability to see the battlefield while your opponent cannot” (Gery et al. 24).

The number of hacks or attacks on information systems is increasing every day, reinforcing the fact that warfare is currently being waged in the information space/cyber domain via information technology. Gery et al. provide reported hacking attempt statistics to provide insight in the volume of cyberwarfare. In 2017 (Gery et al. 23):

- The Pentagon reported 10 million attempted attacks a day;
- The National Nuclear Security Administration also reported 10 million daily hacking attempts;
- The United Kingdom reported 120.000 cyber incidents per day (similar to the amount the State of Michigan deals with);
- The State of Utah reports 20 million daily attempts, which is a considerable increase when compared to two years earlier, when it faced 1 million hacking attempts a day.

One of the biggest issues with current cyber- or information war(fare), alongside the difference in conceptualisation between Russia and the West lies directly in the word ‘war’. As explained above, war has historically mostly been measured by kinetic outcomes such as numbers of deaths, destroyed buildings and infrastructure, conquered lands, etc. Although cyber activities can have kinetic outcomes, such as the causing of power outages that affected 225,000 Ukrainian citizens by launching cyberattacks against three different distribution centres of an Ukrainian power company (Department of Homeland Security), many cyber operations, such as the hacking of government computers are non-kinetic in nature, however, the spreading of hacked documents, misinformation or disinformation can be damaging for a state both. It remains hard to determine however, whether these actions can and should be seen as acts of war or not, especially since it is often hard to attribute these acts to a state. In Russian theories about *Gibridnaya Voyna* and new-generation war, these actions are described, but as mentioned earlier, Gibridnaya Voyna is way for political actors to undermine the political stability and legitimacy, and is not considered war by the Russian military top.

For Gerasimov, "the information space opens wide asymmetrical possibilities for reducing the enemy's fighting potential." (Gerasimov 27). The coordinated use of non-military instruments to provoke civil unrest and instil fear to the point of panic, as happened in Crimea, is a good illustration of the theory in action. The information space is the main battlefield in this conception of information warfare, “a battle between states involving only the use of information weapons in the sphere of information models”. It is, simply put, "to wage war without ever announcing it officially" (Haines).

Russia diverges from the West with regards to the concept of information warfare not only in that it includes cyberwarfare. While in the West there appears to be an emphasis on information “operations” as distinct from concrete acts of war, Russian doctrine specifically regards information within the concept of war, defining information warfare as follows: “Confrontation between two or more states in the information space to damage the information systems, processes and resources, which are of critical importance, and other structures, to undermine the political, economic and social system, and effect massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party” (qtd. in Hunter & Pernik 4).

According to the Dutch Military Intelligence and Security Service (MIVD), Russia possesses a variety of (cyber) means to aid conventional military forces. One example can be found in its capability of attacking adversaries’ critical infrastructure through cyber operations. Another example was seen in Ukraine, where Russia used a ‘spy-app’ that Ukrainian artillery officers had on their phone, which provided Russia with information about Ukrainian troop movement (Ministerie van Defensie).

Besides using information warfare to paralyse Command and Control systems, to cause kinetic damage, to spy on adversary’s positions, or to assist the military in general, Russia also uses different means of deterring, compelling or disorienting its adversaries through more soft power-like cyber operations. These can be divided into (Connell & Vogler 17):

1. State funded, pro-Russian news media sites (e.g., RT and Sputnik)
2. Spreading adverse or misleading information on foreign governments via leaks obtained through hacking or cyber espionage
3. Internet “trolls” starting quarrels and upsetting people

While the pro-Russian news media sites arguably have a far greater reach due to the internet, their use can be compared with older disinformation and propaganda tactics of classic information warfare. Russia’s hacking operations and its usage of internet “trolls” however is something which provides useful insight in its current cyber operations.

Russia has often been accused of using hacking groups which would provide it with a covert, mostly deniable option for data and document acquisition, which can be used for both information and disinformation campaigns. One of the most recent and impactful cases can be found in the hacking of the United States Democratic National Committee (DNC) in 2016. A combination of the release of documents acquired through the DNC hack, alongside manipulative trolling campaigns, allegedly show Russian interference in the 2016 presidential elections, with Hilary Clinton's loss often seen as caused by Russia. Two hacking groups are believed to be responsible for the leaked documents from the DNC servers, Fancy Bear (apt 28) and Cozy Bear (apt 29). Both are believed to either be working for, or being direct cyber components of, Russia's military intelligence agency (GRU) and state security service (FSB) respectively (Connell & Vogler 17-18). It appeared that during the DNC hacks the two groups worked independently of each other, as Cozy Bear's intrusion has been identified going back to the summer of 2015, while Fancy Bear's breached the network in 2016, and no collaboration between the two actors, or even awareness of each other's presence, has been identified by cyber security company CrowdStrike who investigated the hack (Aplerovitch). It is believed that Cozy Bear has been able to monitor the DNC's communications, email and chat traffic, while Fancy Bear has gone directly for the DNC's research on Donald Trump (Connell & Vogler 18).

Russia's trolls, while remaining non-attributable, are a more overt tool in Russia's cyber toolkit. They are used for publicly discrediting anti-Russian information on the internet, spreading misinformation and commenting or publishing pro-Russian points of view online (Hunter, Pernik 6). The origin of Russian trolls has roots in Russian domestic policy. The internet was used by the political opposition to get its message out. As the Russian government could not restrict mediums for oppositional speech, or control the opponents access to the internet, the Kremlin appeared to decide to drown the message out with a pro-Kremlin messaging campaign. Troll farms have been established, and paid, by the Russian government where hundreds of people have been employed to spread pro-Kremlin messages to influence domestic politics, and more recently, to discredit anti-Russian information on the international stage (Connell & Vogler 19).

## 6.3. Summary of this Chapter

Contrary to the West, Russia regards cyberspace as part of the information domain, which provides asymmetrical possibilities that can provoke civil unrest and reduce the enemy's fighting potential. With globalisation, increasing interconnectedness, and the increasing importance of the IoT, Russia is convinced that its information domain is constantly challenged by both internal and external actors, and is therefore perpetually fighting an information war. In order to achieve its objectives, Russia uses overt and covert means to achieve both kinetic and non-kinetic effects. Besides its state-led digital mass media platforms, Russia uses "troll armies" and hackers, which allow for manipulation, information gathering, and the spreading of (mis)information, while maintaining deniability.

Cyber capabilities are causing an evolution in the technological character of war, and have been emphasised in both new-generation warfare and hybrid warfare theories. The question remains, however, whether these means should be addressed as warfare, when they are not accompanied by conventional military means (e.g.: Russian interference in the 2016 US elections). It is perhaps best summarised by General Makmut Gareev, stating that “if an employment of any non-military means is a war, then the whole of human history is ‘war’, as the ‘over-free employment of such a word as “war” devalues the severe [nature of this] concept and dulls its adequate perception in society” (qtd. in Fridman 158).

# 7. Conclusions

The core research question of this thesis was whether hybrid warfare is a viable term with regards to Russia in the current security environment. It may come as no surprise that also the answer to this question is hybrid. In the next few (and final) paragraphs I will nevertheless try to formulate the following four conclusions.

## 7.1. Hybrid Warfare as an Umbrella Term Leads to Misunderstanding and Mystification

Russia's perceived hostile stance regarding the West has been described with a large variety of concepts, of which the notion of hybrid warfare is currently most used. Although hybrid warfare in its original conceptualization was meant to describe the tactical and operational level limited to a spectrum of military or kinetic means, it has outgrown its original definition and is now often used to describe a strategy combining both military and non-military means. Even although most academics, policy-makers and strategist now use such a broader definition of hybrid warfare, a consensus is still lacking.

Since the Ukraine crisis the concept of hybrid warfare has largely, but not solely, been linked to Russia, using the annexation of Crimea, but also the hacking of the DNC, as examples of Russian hybrid threats. With its broad usage, the term (Russian) hybrid warfare has been politicised, whereby every perceived hostile act can be placed in the same conceptual framework, which ensures a continuity in political narrative and allows different domestic actors to unify against an external threat. This has led to militarized narratives reminiscent of the Cold War in both Russia and the West.

The notion of Russian hybrid warfare does however often not correspond with Russia's own contemporary theories regarding war. In Russian military circles hybrid war, or as it is called *Gibridnaya Voyna*, is used to describe Western actions against Russia. In addition, *Gibridnaya Voyna* is not considered to be actual war, as it is made up of non-military, subversive, means. Instead, contemporary Russian military doctrine is better described by new-generation warfare, which does combine military and non-military means, but contrary to Western hybrid war theories, relies heavily on conventional military power. While Frank Hoffman's theory of hybrid warfare, newer Western conceptualizations of the term, *Gibridnaya Voyna* and new-generation warfare can all be used to describe elements of the Ukraine crisis, none of them alone suffice when describing the current situation in the international security arena. In addition, it can be noted that Russia's actions in Ukraine, as described by Karber, were case-specific, and are not sufficient to define Russia's strategy as a whole. It is not fruitful to analyse contemporary Russian threats by placing them under the umbrella of Russian hybrid warfare, and to see this as a grand strategy that drives Russian foreign policy.

## 7.2. Binary Thinking on War and Peace is Outdated

A second conclusion that can be drawn about hybrid warfare, and similar concepts such as gray-zone warfare, *Gibridnaya Voyna* and new-generation warfare, is that it is not only of importance whether the terms are clearly defined, whether there is consensus on their meaning, and whether the usage of these types of warfare is acknowledged. The importance is that these terms show that too many politicians and military personnel are stuck in a black and white distinction between war and peace when a country is at peace, it follows a set of rules and policies, and when it is at war, it follows a different set of policies and rules. If the country is (possibly unknowingly) faced by an adversary who does not consider this distinction binary, being active in some sort of gray zone, a country can lose a game (meaning competition or conflict) that it is not even playing. A metaphor for this creeping normality is the "death by a thousand cuts" or the "boiling frog", whereby a victim is unaware of the harm done by an opponent until it is too late. The danger lies in the outdated idea that there is either war, or there is not, while an opponent might regard the international stage, and international relations as an ongoing competition in all its hybrid and shadowy (gray) forms.

## 7.3. Suitable Reactions to Hybrid Threats are Gray

When considering Russian actions and perceived threats in the international arena, the following should be taken in to account for a suitable reaction: a reaction should *not* be from the binary peace-war perspective, but must be well-aligned to the Russian mindset, which sees the international security arena as a constant competition in which the struggle within the (cyber)information space is unending. When using the concept of the concept of hybrid warfare, anything can be seen or used as a form of war, similar to the notion of unrestricted warfare. This broad umbrella can support dangerous political narratives, while simultaneously providing more confusion than clarification for the military to work with.

## 7.4. Policymakers and Military Leaders Need a New Frame of Thinking

A distinction such as John Chamber's division between gray-zone hybrid threats and open-warfare hybrid threats (figure 2) may prove more useful than one all-encompassing hybrid warfare theory. Using a similar distinction provides policymakers and military leaders with a conceptual framework in which information warfare (increasingly consisting of cyber operations), political warfare consisting of non-military means and conventional military actions (although supported by non-military means) are options to be distinguished. It is important to note that such a model should not once again form a set of binary distinctions, but instead is better viewed as a gradual scale on which Russia or other potential adversaries can be encountered. To prevent disproportionate reactions and escalation a consensus will have to be found with regards to when (cyber)information operations should be considered actual acts of war.

# 8. Bibliography

Alperovitch, Dmitri. “Bears in the Midst: Intrusion into the Democratic National Committee”.  Posted 15 June, 2016.  *Crowdstrike blog.* https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Barno, David. "The Shadow Wars of the 21st Century." *War on the Rocks, 23* July, 2014. warontherocks.com/2014/07/the-shadow-wars-of-the-21st-century/

Bartles, Charles K. "Getting Gerasimov Right." *Military Review* 96.1, 2016, pp. 30-38.

Bensahel, Nora. “Darker Shades of Gray: Why Gray Zone Conflicts Will Become More Frequent and Complex.” *Foreign Policy Research Institute, 5 February* 2016. *www.fpri.org/*article/2017/02/darker-shades-gray-gray-zone-conflicts-will-become-frequent-complex/

Bērziņš, Jānis. "Russia’s new generation warfare in Ukraine: Implications for Latvian Defense Policy." *Policy Paper* 2, 2014. https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

Brands, Hal. "Paradoxes of the Gray Zone." *Foreign Policy Research Institute*, February 5, 2016. *www.fpri.org/*article/2016/02/paradoxes-gray-zone/

Bruusgaard, Kristin Ven. "Crimea and Russia's strategic overhaul." *Parameters* 44.3, 2014, p. 81. www.questia.com/library/journal/1G1-397579205/crimea-and-russia-s-strategic-overhaul

Callard, James, and Peter Faber. "An Emerging Synthesis for a New Way of War: Combination Warfare and Future Innovation." *Georgetown Journal of International Affairs*, 2002, pp. 61-68. https://www.jstor.org/stable/43133476

Chambers, John. *Countering Gray-Zone Hybrid Threats: An Analysis of Russia's New Generation Warfare and Implications for the US Army*. US Military Academy-Modern War institute West Point United States, 2016. https://mwi.usma.edu/countering-gray-zone-hybrid-threats-mwi-report/

Chekinov, S. G. and S.A. Bogdanov. “The Nature and Content of a New-Generation War”. *Military Thought (Военная Мысль*), No. 10, 2013, pp. 13-25.

Chivvis, Christopher S. "Understanding Russian Hybrid Warfare." Rand Corporation, 2017. www.rand.org/pubs/testimonies/CT468.html, DOI: https://doi.org/10.7249/CT468

Clausewitz, Carl Von. *On War.* Translated by Miss Maguire, with notes by T. Miller Maguire. William Clowes, 1909 (first German edition “Vom Kriege” consists of 8 books, published since 1832). https://archive.org/details/in.ernet.dli.2015.278730/page/n1. ark:/13960/t9g50160f

Connell, Michael and Sarah Vogler. “Russia's Approach to Cyber Warfare”. *Occasional Paper, Center for Naval Analyses, Arlington, VA,* 2017. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

Davis Jr, John R. "Continued evolution of hybrid threats." *The Three Sword Magazine* 19.28, 2015. infosec-journal.com/article/continued-evolution-hybrid-threats-russian-hybrid-threat-construct-and-need-innovation

Department of Homeland Security, “Cyber-attack against Ukrainian Critical Infrastructure”, 25 Febuary, 2015. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

DeWees, Bradley, et al. “Toward a Unified Metric of Kinetic and Nonkinetic Actions: Meaning Fields and the Arc of Effects”. *Joint Force Quarterly, Issue 85, 2nd quarter,* 2017. ndupress.ndu.edu/Publications/Article/1130645/toward-a-unified-metric-of-kinetic-and-nonkinetic-actions-meaning-fields-and-th

Dosse, Stéphane. "The Rise of Intrastate Wars: New Threats and New Methods." *Small Wars Journal,* 25 August, 2010. https://smallwarsjournal.com/jrnl/art/the-rise-of-intrastate-wars

Duggan, Patrick. "Man, Computer, and Special Warfare." *Small Wars Journal. January* 4, 2016, 12:21pm. https://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare

Felgenhauer, Pavel “A New Version of the ‘Gerasimov Doctrine’?” *Eurasia Daily Monitor.* Vol. 16, Issue 32. March 7, 2019 06:22 PM. https://jamestown.org/analyst/pavel-felgenhauer/

Fridman, Ofer. *Russian" Hybrid Warfare": Resurgence and Politicization*. Oxford UP, 2018. https://DOI.org/10.1093/oso/9780190877378.001.0001

Galeotti, Mark. "Hybrid, ambiguous, and non-linear? How new is Russia’s ‘new way of war’?", *Small Wars & Insurgencies* 27.2, 2016, pp. 282-301. https://doi.org/10.1080/09592318.2015.1129170

Galeotti, Mark. "Hybrid war” and “little green men”: How it works, and how it doesn’t." *Ukraine and Russia: People, politics, propaganda and perspectives* 156, 2015. https://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/

Galeotti, Mark. “I’m Sorry for Creating the ‘Gerasimov Doctrine’.“ https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Galeotti, Mark. "The ‘Gerasimov doctrine’ and Russian non-linear war." *Moscow’s Shadows* 6, 2014. http://cs.brown.edu/people/jsavage/VotingProject/2017_03_09_MoscowsShadow_GerasimovDoctrineAndRussianNon-LinearWar.pdf

Gerasimov, Valery. "The Value of Science is in the Foresight." *Military Review* 96.1, January-February, 2016, p. 23 (originally published in Russian in 2013). www.scribd.com/document/363743920/Academic-OneFile-Document-The-Value-of-Science-is-in-the-Foresight-New-Challenges-Demand-Rethinking-the-Forms-and-Methods-of-Carrying-Out-Combat-O

Gery, William R., SeYoung Lee, and Jacob Ninas. "Information Warfare in an Information Age." *Joint Force Quarterly, Issue 85, 2nd quarter*, 2017, pp.22-29. https://ndupress.ndu.edu/Media/News/Article/1130649/information-warfare-in-an-information-age/

Giles, Keir. "Russia’s toolkit’." *Keir Giles, Philip Hanson, Roderic Lyne, James Nixey, James Sherr and Andrew Wood, The Russian Challenge, Chatham House Report*, 2015, pp. 40-49. https://www.researchgate.net/publication/280611569_Russia's_Toolkit

Haines, John R. "Russia’s Use of Disinformation in the Ukraine Conflict." *Foreign Policy Research Institute: E-Notes*, 2015. https://www.fpri.org/contributor/john-haines/

Hillson, Roger. *The DIME/PMESII model suite requirements project*. Naval Research Lab Washington DC Information Technology Div., 2009, pp. 235-239. https://apps.dtic.mil/docs/citations/ADA525056

Hoffman, Frank G. *Conflict in the 21st century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies, 2007. https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Hoffman, Frank. "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats." *War on the Rocks,* July 28, 2014. https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

Hunter, Eve, and Piret Pernik. *The challenges of hybrid warfare.* International Centre for Defence and Security, 2015. https://icds.ee/the-challenges-of-hybrid-warfare/

Karber, Phillip A. “Russia's 'New Generation Warfare'.” *National Geospatial-Intelligence Agency*, 4 June 2015. www.nga.mil/MediaRoom/News/Pages/Russia%27s-%27New-Generation-Warfare%27.aspx

Kukkola, Juha, Mari Ristolainen, and Juha-Pekka Nikkarila. "GAME CHANGER Structural transformation of cyberspace."*: Finnish Defence Research Agency*, Puolustusvoimien tutkimuslaitos, 2017. https://www.researchgate.net/publication/321767657_GAME_CHANGER_Structural_transformation_of_cyberspace

Liang, Qiao and Wang Xiangsui, *Unrestricted Warfare.* PLA Literature and Arts Publishing House, February 1999. https://archive.org/details/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui ark:/13960/t4dn8652w

Markoff, John. "Before the gunfire, cyberattacks." *New York Times* 12, 2008, pp.27-28.

Mazarr, Michael J. *Mastering the gray zone: understanding a changing era of conflict*. US Army War College Carlisle, 2015. https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303

McDermott, Roger. "Gerasimov Unveils Russia's 'Strategy of Limited Actions'". *Eurasia Daily Monitor.* Vol. 16, Issue 31, March 6, 2019 02:41 PM. https://jamestown.org/analyst/roger-mcdermott/

Milevski, Lukas. "Respecting Strategic Agency: on the categorization of war in strategy." *Joint Force Quarterly* 86, 2017, pp. 35-40. https://www.academia.edu/33690018/Respecting_Strategic_Agency_On_the_Categorization_of_War_in_Strategy

Ministerie van Defensie/ Militaire Inlichting- en Veiligheidsdienst. "Hybride oorlogvoering", *MIVD Jaarverslag 2016, Specials 01,* April 24th, 2017. https://magazines.defensie.nl/specials/2017/01/02_wij-zijn-de-mivd

Monaghan, Andrew. "The 'War' in Russia's' Hybrid Warfare'." *Parameters,* 45.4, 2015, p. 65.

Pettersson, Therése and Kristine Eck. "Organized violence, 1989-2017." *Journal of Peace Research* 55(4), 2018. https://journals.sagepub.com/doi/10.1177/0022343318784101

Renz, Bettina, and Hanna Smith. "Russia and Hybrid warfare-going beyond the label." Kikimora P, 2016. https://www.stratcomcoe.org/bettina-renz-and-hanna-smith-russia-and-hybrid-warfare-going-beyond-label

Schadlow, Nadia. "Peace and War: The Space Between." *War on the Rocks,* 18, 2014. https://warontherocks.com/2014/08/peace-and-war-the-space-between/

Shapiro, Steven A. and Oliver Davis. “Mission command of sustainment operations”, January 2, 2019. https://warontherocks.com/2016/10/american-strategy-and-the-six-phases-of-grief/

Smith Jr, Paul A. *On political war*. National Defense University Washington DC, 1989. https://apps.dtic.mil/dtic/tr/fulltext/u2/a233501.pdf

Staff, The Joint Chiefs of, “Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms,” June 2015. https://www.hsdl.org/?abstract&did=750658

Thomas, Timothy. "The evolution of Russian military thought: Integrating hybrid, new-generation, and new-type thinking." *The Journal of Slavic Military Studies* 29.4, 2016, pp. 554-575. https://doi.org/10.1080/13518046.2016.1232541

Votel, Joseph L., et al. "Unconventional warfare in the gray zone." *Joint Forces Quarterly* 80.1, 2016, p.101. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/

Weitz, Richard. "Countering Russia’s Hybrid Threats." *Diplomaatia,* 21 November, 2014. https://icds.ee/countering-russias-hybrid-threats/