University of Peloponnese
Faculty of Social and Political Sciences
Department of Political Studies and International Relations

Master Program in

Mediterranean Studies

Hybrid Threats: A new menace in International Era and the Presence of Russia in the Balkan Peninsula

Toumpani Margarita Georgia

Corinth, Greece, January, 2019

Hybrid Threats: A new menace in International Era and the Presence of Russia in the Balkan Peninsula

Keywords: hybrid threats, hybrid warfare, Russia, Balkans, strategy, influence

Abstract

This dissertation addresses a questions' set; what a hybrid threat is? Does Russia has hybrid strategy and if yes, which are its characteristics? Does Russia applies such strategy against the Balkans? The main research problem, in which the question is referred, is the delimitation of hybrid threats and Russia's hybrid strategies in the Balkans.

The methodology we are going to follow is the qualitative method, using references from the theory of international relations, the field of strategic studies, geopolitics and history. In the essay after the definition of hybrid threat, we argue that Russia has hybrid strategy, by analyzing it and by giving recent examples.

In the first chapter we analyze and clarify the term "hybrid threat", in the second, Russia's hybrid strategy in theory and in the third some cases of Russia's hybrid strategy in the Balkans. In the section of conclusions, there are the results of the findings and author's opinion.

With this statement:

1. I expressly and unambiguously declare that my dissertation thesis is a product of my own intellectual effort, does not violate third parties' rights and follows the internationally recognized standards of scientific writing, faithfully adhering to academic ethics.
2. The opinions expressed are solely the responsibility of the author and the supervisor, the examiners; the Department and the University of Peloponnese do not necessarily adopt the expressed views or bear any responsibility for any errors and omissions.

Table of Contents

List of Abbreviations & Glossary

Abbreviations

Apt28 – Advanced Persistent Threat 28 – Russian hacker's group

DDos – Distributed Denial of Service – type of cyber attack

EU - European Union

NATO – North Atlantic Treaty Organization

RT – Russia Today – Russian Media

RBTH – Russia Beyond the Headlines – Russian Media

Glossary

Click-baits: Attractively designed thumbnail link, which is leads the user who clicks it in another website or in a linked online content.

Ddos attacks: It is as malicious that tries to disrupt the normal traffic and function of the server which is under attack.

Phishing attacks: A covered online entity or action (e.x. an e-mail), which looks reliable but it, has a target to intercept personal data and private and sensitive information.

List of Tables

Introduction

The world is experiencing radical changes as decades pass by and states are trying to find alternative ways in order to have positive results from their decisions, for their own benefit. Different strategies and different interests are forming and all these together create a mixture of new terms that need to be examined. One of these new-entry terms is “hybrid threat”; thus a non-conventional way to pose threat against another state.

The term of hybrid threat became mainstream after Russia’s actions in its neighboring countries, Ukraine and Georgia and non-neighboring, the Balkan states. After these events, international security agencies focused on Russia's advanced strategy, aiming to find ways to deal with this new challenge. Another essential cause was that Russia had Soviet past on such techniques and had experience on using hybrid tools. Last but not least, and maybe most importantly, another reason that made this term famous was that Russia posed a new idea of danger, through its threats; Putin's Russia attempts to make Russia a great power again with a larger territory and more significant influence, against the Western countries.

The main research question has to do with the correlation of hybrid threats, corresponding to Russian strategies. Thus the question is what are a hybrid threat and a hybrid war, which is Russia's hybrid strategy and which are the hybrid threats Russia has already posed in Balkan countries, in order to serve its national interests in the wider area? In other words, the question has three parts; to provide a defining area for the term hybrid threat and its gradations or escalation (hybrid conflicts, hybrid wars), to analyze Russia's hybrid strategy and to observe recent cases of Russia's application of these strategies.

Wherefore the term of hybrid threats is vague and broad and having in mind that Russia's strategies are not limited in its neighboring countries or generally in those who are closer, the question is focused on the situations occurred in the Balkans.

In order to fully comprehend the term “hybrid threat” we will also examine the escalating situation where a threat becomes something more; the “hybrid warfare”.

In this dissertation, we argue that Russia clearly has a hybrid strategy and poses hybrid threats to other countries, especially in the Balkan Peninsula. This way of analysis does not show any anti –Russian or pro-Russian tendencies. For this reason, we will try to make our analysis by approaching the subject with as much neutrality as possible. Moreover, we will give some examples of events in the region during the 21st century, when Russia used hybrid strategies to achieve its goals and increase its influence.

Additionally, the appropriate way to observe and analyze the subject is by using a qualitative research method. To make our research method easier, we will also use in the last section of the dissertation, a case study design model. Through cases of the modern history, and by using the theory of realism in international relations, geopolitics, history and strategy as tools, we will examine Russia's actions in other countries, and we will clarify the meaning of hybrid threats. Even though the analysis has as time horizon the 21st century, for explanatory purposes we will use some examples from the past though, these examples we will be limited and brief.

Starting the first chapter of this dissertation, we will try to analyze the term of hybrid threats. For this delamination, we will use definitions of strategists and academics in order to better understand the term and to set the basis for next chapters' analysis. Furthermore, there will be a conceptual comparison with other types of threats, such as the asymmetric ones, aiming to be more precise and give as integrated definition as a possible of the term. After analyzing hybrid threats, we will see the escalation of the hybridity a situation can have; from hybrid threats to hybrid conflict and finally to hybrid warfare.

Going forward to the main subject of the dissertation, in the second chapter we will attempt to analyze all types of hybrid strategy Russia has adopted throughout the years, from 2000 until now. In an entirely theoretical context, we will analyze the types of Russia's hybrid threats, under which circumstances, according to bibliography and modern history, Russia uses hybrid threats against other countries and who are its targets, by identifying its aims, instruments and the "hybridity" in its actions.

Last but not least, in the third chapter, we will examine five case studies from the Balkans, that Russia posed hybrid threats and strategies, in order to expand its influence in the region. Needless to say that through these examples we argue that Russia posed hybrid threats against other countries, even if in some cases Russia never confirmed or accepted these arguments officially.

To sum up, the dissertation examines the term “hybrid threat” from 2000 until now, the hybrid strategy of Russia and the hybrid threats Russia poses in Balkan countries. The main argument is that Russia has indeed a hybrid strategy, which imposes against Balkan countries, in the majority of modern cases and there is a definition and a delimitation of the term “hybrid threats”.

CHAPTER 1: Hybrid Warfare and threats: Challenges of the 21st century

The concept of ‘hybrid threats’ is not a new entry in the international relation’s terminology. It has appeared with different “words” expressed by various organizations, from the new millennium until now. Despite the diversity of names, in all cases, it seemed to be the same thing and a threat with the same -or almost the same- characteristics and simultaneously with no specific characteristics. As we will analyze below, the term “hybrid threat” is an umbrella term because it combines many different tactics and instruments, creating a new “entity” with familiar shape and tools (Miklaucic, 2011).

In this paper, we will concentrate our analysis in the 21st century’s hybrid threats. However, it should be mentioned that the idea of hybrid threats, shaped in the form of the use of non-military means, is dated back to the ancient Greece and the Peloponnesian War[1] (Sari, 2017, p. 9) (Mansoor, 2012, pp. 3-4).

In the modern era of the 21st century, with the great advances of technology, the first tangible situation of hybrid threat appeared by a non-state actor, Hezbollah, during the 34-day Second Lebanon War in 2006. There was a profound domination of Hezbollah, against the Israeli Defense Forces (IDF). The tactic Hezbollah used, seemed to be psychological warfare; this type has to do with the use of non-violent conflict methods, such as persuading target audiences, concentrating in the country’s home audience, where their actions should be justified (Schleifer, 2006, p. 2). Moreover, in this way, we can argue that this conflict is in the list of “modern asymmetric conflicts” (Schleifer, 2006, p. 16).

[1] In the Peloponnesian War, in a conflict between Athenians and Spartan, the second decided that they should keep some military forces also in their homeland in order to prevent a revolt from the Helots (subjugated population in Sparta, like slaves, who worked in the agricultural sector and supported the Spartan military system). The Athenian strategy also included the creation of ideal situation for Helots’ revolt. In 425 BC, Athenians fortified with their forces Pylos with Messenians of Naupactus (their ancestors had expelled by the Spartans) Helots began to abandon the area and Spartan had to face an emergency situation there, because they could not use their phalanxes. This was a type of hybrid strategy in the ancient world.

In a more formal context, hybrid threats raised concerns in 2010 within NATO. The new Strategic Concept of 2010 first reflected the definition of hybrid threats, which incorporated in the NATO Capstone Concept. According to this definition, hybrid threats are "*those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives"* (North Atlantic Treaty Organization, 2010, p. 2). As referred, hybrid threats became a significant challenge for the Alliance.

In the latest NATO Summit Guide in Brussels, in July 2018, there is a chapter dedicated to Organization's response to hybrid threats. There is also a reference to some hybrid methods, such as *non-military tactics, deception, propaganda, and sabotage*, as well as to hybrid threats NATO faces and Organization's strategy (North Atlantic Treaty Organization, 2018, p. 73).

The US Defense Counsel, Frank Hoffman also gives a definition of hybrid threats. According to his definition "*hybrid threats are consist of tactics, which opponent sides apply simultaneously and through intertwined engagement of conventional weapons, non-conventional tactics, terrorism, and criminal behaviors at the same place and at the same time, aiming to conquer their political objectives*" (Hoffman, 2014).

Threats against a country can be both direct and indirect and can affect the state in a political and a national level, as well. In the EU level, during the Latvian presidency in 2015, the EU Defense Ministers, in an informal meeting in Riga, discussed the revision of the European Security Strategy and they called for unity, triggered by modern crises, concerning Union's security, in all levels (Pawlak , 2015, pp. 5-7). The same year, in May, European External Action Service distributes a food-for-thought paper with the title "Countering Hybrid Threats" (European External Action Service (EEAS), 2015). The central concept around this was EU's inherent to recognize a possible threat and build resilience around it.

Recently, on February 26th, 2018, European Parliament discussed the subject of "Countering Hybrid Threats: EU and the Western Balkans Case" (Countering hybrid threats: EU and the Western Balkans case, 2018). In this meeting, they presented the multi-layer concept of hybrid threats, in a revised version and how Russia's declining influence affects the main area of Western Balkans. Since then, the EU used the term "hybrid threats" in order to define the difficulties posed by non-European influencers in the central area (ex. Russia, Turkey, Saudi Arabia).

Meaning and Clarification of Hybrid Threats

To start with, we need first to define what we mean with the word ‘‘hybrid". According to Merriam-Webster, the adjective ‘‘hybrid’’ is something *heterogeneous in origin, in composition or appearance; having or produced by the combination of distinct elements, two or more* (Merriam-Webster (n.d.), n.d.).

However, it is still difficult to define what hybrid threats are. In the field of defense and security hybrid threats are divided into four levels (Countering hybrid threats: EU and the Western Balkans case, 2018, p. 9). This demarcation is due to their concerns, priorities and their idea about hybridity, in general. Based on them, first there is the political level. In this level, the state or the non-state actor has the option to choose to unsettle the international order by challenging other actors on purpose and by force. When we say "force", we mean that the actor acts against others will.

As we already mentioned, "hybrid threat" is an umbrella term synthesized by existing adverse situations. Such situations can be, for example, a migration phenomenon for various reasons, ethnic conflicts regardless of the nation or the region, piracy or corruption. Another element of hybrid threats, which is entirely new, is that there is a systematic and adaptive use of instruments or tools (combined or not) in order to achieve long-term political objectives (Miklaucic, 2011). The exciting thing about this type of threats is that it does not require a new way of thinking or new abilities and capabilities[2] because it is something more than a total of constituent parts.

On the second level, the strategic one, there is a variety of tactics. Specifically, there is a combination of both direct and indirect strategies, from all possible fields, such as diplomacy and economy, by using all available information technologies (ex. cyber) (Countering hybrid threats: EU and the Western Balkans case, 2018, p. 9). The third

[2]. Many of these threats are the consequences of underlying problems in a society, such as poverty, ethnic strife, and other similar examples.

level is the operational one. There, conventional and non-conventional capabilities use weakening strategy. Such capabilities are for example area denial and weapons of mass destruction. Last but not least, the fourth level is the tactical one. On this level someone can include terrorism; it has to do with irregular actions by using conventional and non-conventional means (Countering hybrid threats: EU and the Western Balkans case, 2018, p. 9).

Delimitation of hybrid threats

Starting with the general concept of “threats”, there are many different. These types can be hybrid or asymmetric, internal or external, environmental, nuclear, with military or diplomatic dimensions (Brauch, 2011, pp. 63-64). Despite the fact that in the majority of these types of threats we can find their differences, many people are confused between hybrid and asymmetric threats.

In order to understand better the difference between the asymmetric and hybrid threats, we need to give definition of the first term. Asymmetric threats include the element of surprise and unexpected action; it is, in other words, a way of fighting unfairly. In all dimensions of asymmetric threats, operational and strategic, the weapons are used in a not scheduled way. It also includes the designing strategy by an opponent, which prepares the ground for the conflict (Binnendijk, 1998, p. 169). So, we can say that the main difference between the two has to do with the use of military force.

There are also three other important things that characterize hybrid threats and differentiate them form the other threats. Firstly, in hybrid threats the combination of tools from multiple fields make them hard to be detected. Secondly, the use of hybrid threats create non-linear effects, which makes them unforeseeable with overwhelming results. And thirdly, they create vague situations and unclear predictions for the other side, that make easier for the one who applies them to act quickly and to change its objectives, targets or the tools he uses, contextually the progress of a situation (Treverton, Thvedt, Chen, Lee, & McCue, 2018, p. 60).

From Hybrid threats to hybrid conflict and hybrid warfare

Taking into consideration the intensity of a situation or the use of means a classification can be made between hybrid threats, hybrid conflicts, and hybrid warfare (Pawlak , 2015, p. 1). In order to understand the classification, it is first important to have in mind that hybrid threats, in general, have to do with the interconnection or the convergence of multi-dimensional factors and different elements. A state or a non-state actor, so that to achieve its strategic aims, uses hybrid tactics, such as informational warfare, economic tools, or influencing internal ethnic groups etc. The other two, hybrid conflict and warfare, are different phenomena in which the opponent parties utilize hybrid threats through specific tactics, in order to satisfy their objectives.

In the case of hybrid conflicts parties avoid using military force against the other opposing parties; even though there are also some brief incidents as exceptions. In contrast, they blend all actors and all their available means such as military intimidation, use of economic-political, technological, diplomatic means and humanitarian aid (Pawlak , 2015, p. 2).

Actors through the use of hybrid threats can lead to different results such as economic destabilization, humanitarian crises, doubts on behalf of citizens for their government and physical jeopardizing of opponents. However, the particular side of hybrid threats are revealed when one of the sides involves either the 'entity' itself, criminals, or criminal groups in cooperation with military or even paramilitary forces (Countering hybrid threats: EU and the Western Balkans case, 2018, p. 29). Back in 2008, during the Russian-Georgian conflict, Russia involved a large number of criminal actors in the area of South Ossetia, within the context of the idea of ethnic cleansing of this part of the country by the Georgian population.

The threat becomes a war

As we already mentioned, there are also different terms to describe a hybrid threat that is dependent on the intensity or the outbreak of an event. As a hybrid conflict can be described an event where the enmeshed parties do not use direct armed forces, but they prefer combined methods. Such methods are technological or diplomatic in order to achieve their objectives, military intimidation or the exploitation of other's party vulnerabilities, both political and economic (Countering hybrid threats: EU and the Western Balkans case, 2018, p. 31).

As a situation continuous escalates, it can be transformed from hybrid conflict to a hybrid war. The concept remains almost the same, as the ‘hybridity' depends on the use of means; the actor in a hybrid war does not refrain from an undisguised use of armed forces, but it also includes a mix of alternative means, such as political, diplomatic or economic "weapons." Furthermore, in a hybrid war situation, the parties, alongside the use of the abovementioned means, also use their armed forces openly (Pawlak , 2015, p. 1).

Defining Hybrid Warfare

According to Merriam-Webster warfare consist of *military operations between enemies and an activity undertaken by a political unity, such as a country or a nation, aiming to weaken or destroy another actor in the system* (Merriam-Webster (n.d.), n.d.).

However, the strategist Carl von Clausewitz has also given in 1832 the definition of warfare. According to his definition “*war is a mere continuation of politics by other means”* (Clausewitz, 1984, p. 28). Taking into consideration the work of Clausewitz and combining it with the abovementioned theory we will be able to understand what hybrid warfare is. The strategists give answers on the subject based on the Napoleonic Wars, giving three criteria, an aggressive action should have in order to be characterized as warfare. Having in mind the theory of Clausewitz, Thomas Rid summarizes these characteristics on violence, political and instrumental (Rid, 2012, p. 7).

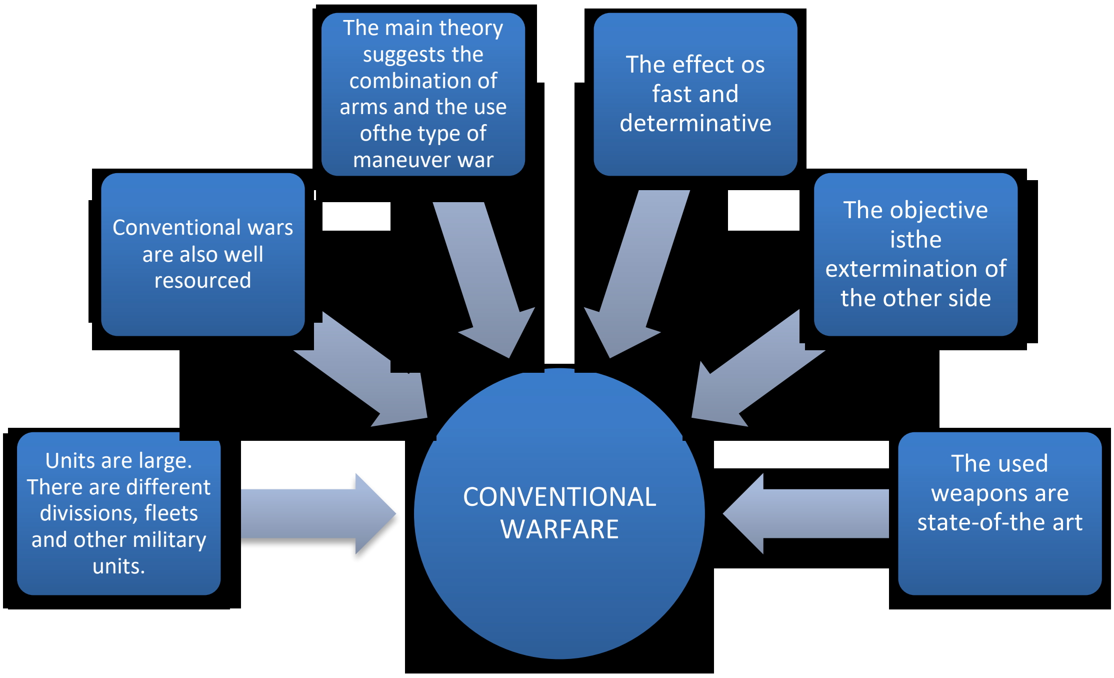
To start with this analysis, according to the first criterion warfare, in its nature, consists of acts of force, *id est* is violent and in this shape can oblige the other side (the enemy) to our aims and will. The second criterion, the political, has to do with the nature of the goal (the political one) that warfare has. The third criterion is warfare's instrumental character. Hence, the means used in the warfare should serve its objective political goals; they should act in a way to achieve them and is never disoriented from the primary purpose. It is also clear that the abovementioned should exist, at least, on the one side of the conflict (Clausewitz, 1984, p. 28) (Rid, 2012, p. 7). The work of Clausewitz is still considered to be the milestone on the military theories of Western World (Andersen, 2012, p. 22) and as a result, his theories and his work are incorporated in the term of "*conventional warfare*" (Wilkie, 2009, p. 14).

Moreover, in the framework of conventional warfare, according to Reyeg and Marsh, conventional warfare capabilities are usually related to a country's military instruments such as an army's big units, aircraft, naval forces, and the combination of armed forces with maneuver warfare (Reyeg & Marsh, 2011, p. 5). In recent years, there are many academics that do not agree with the theory of Clausewitz because they think that it is not up to date and do not think that is relevant to 21st century's warfare models. According to these contemporary academics, specialized in the military theory, projected examples from 1990s wars in Africa (Somalia and Rwanda) and in the Balkan Peninsula (Schuurman, 2010, p. 89) combine elements of both regular and "irregular" conventional warfare (Lanoszka, 2016, p. 177)

As in the concept of conventional warfare, the irregular war also has difficulties in the definition. In irregular warfare, there are three criteria that help us to recognize it. In this type of small warfare, units of military forces apply tactics that are used in guerillas and terroristic tactics, as well. (Arquilla, 2011, pp. 4-6).

Furthermore, innovation and creativity are not absent in irregular wars, due to the confined quantity of resources; and for this reason, it becomes essential to develop a new way of thinking, for creating new strategies. All these new parameters increase the risks in such situations because there is no ability to directly confront the conventional type (Reyeg & Marsh, 2011, pp. 6-7). In the tables below we will see the characteristics of both irregular and conventional warfare in the form of comparative analysis, in order to better understand these difficult concepts.

Table 1.1 Characteristics of Conventional War



The main theory suggests the combination of arms and the use ofthe type of maneuver war

The effect os fast and determinative

Conventional wars are also well resourced

The objective isthe extermination of the other side

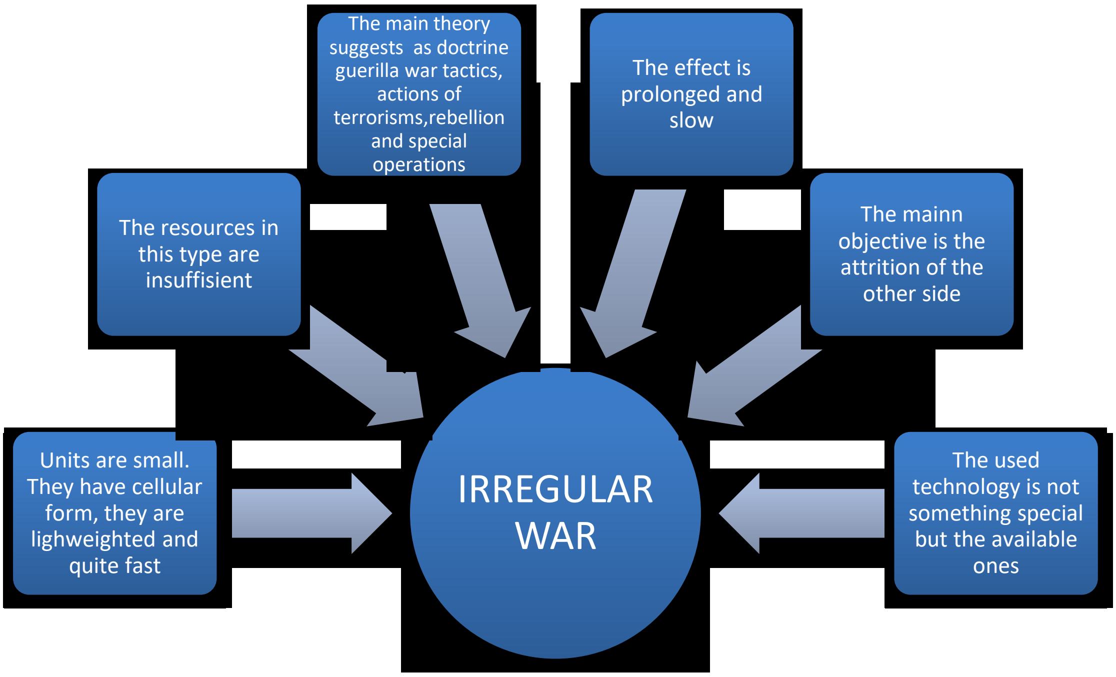
Units are large. There are different divissions, fleets and other military units.

CONVENTIONAL WARFARE

The used weapons are state-of-the art

Source for the data: (Reyeg & Marsh, 2011, p. 9)

Table 1.2 Characteristics of Irregular War



The main theory suggests as doctrine guerilla war tactics, actions of terrorisms,rebellion and special operations

The effect is prolonged and slow

The resources in this type are insuffisient

The mainn objective is the attrition of the other side

Units are small. They have cellular form, they are lighweighted and quite fast

IRREGULAR WAR

The used technology is not something special but the available ones

Source for the data: (Reyeg & Marsh, 2011, p. 9)

Examples of Hybrid situations in the Modern Era and the Challenges in the global security

In the modern era, there are many examples of hybrid threats that help us understand this concept better. It is essential though to understand that, those hybrid threats are multidimensional, globally interconnected, adaptable and integrated into the local communities or population and quite innovative and enterprising (Gashi & Maqedonci , 2017, p. 92).

In the latest events of the 20th century, one example of hybrid war is found in the War of Vietnam, where the Vietnamese side (Viet Cong and People's Army of Vietnam) used both conventional (regular) and non-conventional (paramilitary) means in order to fight against the French and the US military forces (Gashi & Maqedonci , 2017, p. 93).

Furthermore, the most famous form of hybrid threat is terrorism (Hoffman, 2014). Different terrorist organizations are present across the territories of many states, operating in different fields and using various methods in order to manage their aims and goals. These methods can be economical and military, as well as technological.

Another example of a hybrid threat is cyber security. As technology is rapidly developing, the issue of security through the web is more and more relevant than ever. The main problem with this type of threat is that actors use easily cyber weapons due to the absence of laws and norms concerning the actor's behavior in cyberspace. Examples of cyber warfare we can be found in cases of Russia or China. These countries use state-sponsored hackers in order to hinder some other countries in their cyber-space programs (Gashi & Maqedonci , 2017, p. 93).

Another example of a hybrid threat is the scarcity of resources; it is a usual tool of political pressure. A profound case of this example can be found back in 2011 when India refused to adopt an agreement with Bangladesh for sharing potable water, aiming to exercise pressure in their bilateral relations (Gashi & Maqedonci , 2017, p. 94). One year earlier, China refused and prohibited to export raw materials to its neighboring country, Japan. This action was the country's response to Japan because the latter arrested the crew of a Chinese fishing boat (Gashi & Maqedonci , 2017, p.

94). Last but not least, covert operations are also included in the list of hybrid threat examples. The most popular situation is Russia’s tactic against Ukraine by using special secret forces, named ‘the green men’ to spread misleading information. In the third chapter of this essay we will see the dimensions and the forms of Russian hybrid strategies in other Balkan cases.

Countering Hybrid Threats

In order to counter hybrid threats, it is essential to understand how to use the existing capabilities correctly, in an innovative and modern way. The primary purpose is to meet up the new challenges and not the new hardware (Miklaucic, 2011). Talking about this concept that has to do with a comprehensive approach, three subjects emerge. The first one has to do with the full interaction with other actors in the international system, the second one with the coherent enforcement of political tools of power and the third one with the comprehensive elements of crises and actions in all the fields and levels (Miklaucic, 2011).

Even though the abovementioned subjects are emerged, the concept seems to be undeveloped. All the necessary instruments for comprehensive activities (such as the rule of law, governance, economic development, etc.) are traditionally not found in a country's military forces but in Non-Governmental Organizations (NGO's) and the private sector. Also, groups of civilians are sometimes suspicious of the military, or they are not used to cooperate with them (Miklaucic, 2011). However, in a society that faces such threats and challenges, all parts should work together, and civilians should become counterparts and they should also collaborate and cooperate well with each other.

CHAPTER 2 Russia’s Hybrid Strategy

According to Berzins the hybrid strategy of Russia counts on three levels that are interrelated which are allegiance to the idea of legalism, a doctrinal unilateralism, and constant refuse for using open military forces (Berzins, 2014, p. 3). Based on these, the idea of legalism refers to Russia's efforts to justify its actions through law, and this idea of legalism rises from the doctrinal unilateralism that legitimacy can derive from the successful use of force. The last one, the refuse for use open military forces has to do with the diplomatic rhetoric, as used in many recent cases, such this in Crimea.

Russia the last years passed in the modernization of its military forces emphasizing on three main characteristics (Kasapoglu, 2015, p. 4). The first criterion is to equip Russian military forces with modern weapons and army tools, the second one the army to be vigilance and the third one is the upgrade of army's personnel and workforce. Although the first criterion, for modern weapons, is difficult to be defined, because of Russia's different depiction, the second and the third can be explained.

The criterion about the army's vigilance or readiness has to do with its ability to move quickly from its permanent military basis to another, primarily for reasons of the army's protection. The third one, workforce's upgrade has to do with the amelioration of Russian military training and their combat capabilities (Kasapoglu, 2015, p. 4).

The Soviet Past of Russia’s Hybrid Strategic Elements

Hybrid strategy is not as modern as many people believe, especially in Russia’s history. If we take a look in the Soviet era we will realize some roots of "hybridity"; modern Russian hybrid strategy involves techniques and concepts used by the Soviet Union decades ago.

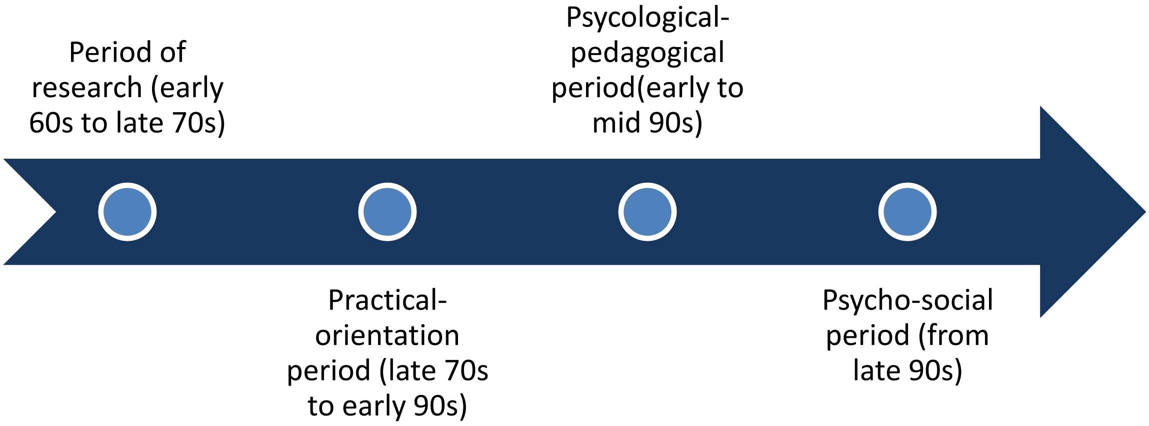
The concept of *Maskirovka* was one of the most famous techniques in the Soviet Military Strategy, as one of Russia’s purposes and part of the central concept of Russia's reflexive control (Thomas, 2004, p. 239) (Kasapoglu, 2015, p. 5).

Maskirovka was named a large-scale deception and disorientation Russian political-strategic campaign, which was characterized by the combination of "friendly" activities toward the West and violent actions.

A brief Theory of Reflexive Control

The theory of reflexive control preexisted the information operations by the military forces and the information warfare, and its developments have passed through four periods of transformation. The table below shows this transformation through the decades, starting from the early 1960s until the late 1990s (Thomas, 2004, p. 238).

Table 2.1 Periods of Reflexive Control



Period of research (early 60s to late 70s)

Practical-orientation period (late 70s to early 90s)

Psycological-pedagogical period(early to mid 90s)

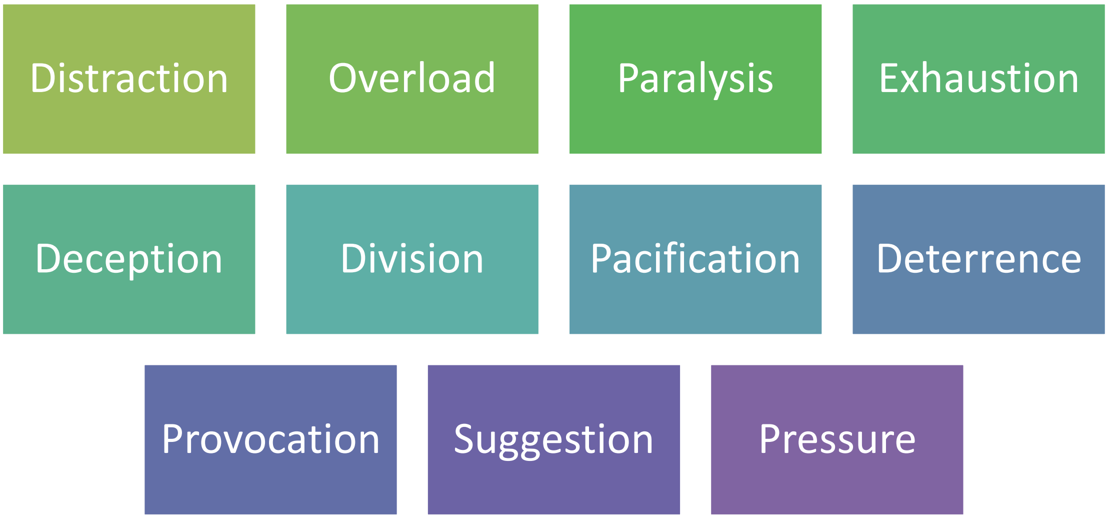
Psycho-social period (from late 90s)

Source for the data: (Thomas, 2004, p. 238)

Many Russian military theorists have written about the impact information has on reflexive control. Major General M. D. Ionov have first written about this concept and have focused on the ways and methods of transmitting a piece of information to the opponent, in order to influence enemy's thinking, to changes his mindset and to achieve control over him. According to him, there are four methods, concerning the information transfer, which can ambush the opponent side (Thomas, 2004, p. 243). The first one is the power pressure by using, among other things, proactive maneuvers and psychological operations. The second method is the disinformation about the situation between the belligerents with subversive activities. Moreover, the transmission of false data which influences opponents decision-making process is another method and the last one is to blindside the enemy by changing the decision making time, aiming the enemy to take rushed decisions and, as a result, to modify operation's character (Thomas, 2004, p. 243).

Emphasizing in the abovementioned methodology, Colonel S. A. Komov wrote about the impact of information warfare over the opponents, (Thomas, 2004, p. 248). The table below summarizes in twelve points Komov's approach for the conduction of information war.

Table 2.2 Komov's Methodology for the Information Warfare



Distraction	Overload	Paralysis	Exhaustion
Deception	Division	Pacification	Deterrence
Provocation	Suggestion	Pressure	

Source for the data: (Thomas, 2004, p. 248)

Distraction: It is achieved when the one side constructs a threat or creates a threatening situation in order to make the opponent rethink about his decisions.

Deception: Using coercive methods against the opponent in order to make him re-distribute his military forces, especially before critical operations.

Provocation: The opponent acts by coercion and his actions benefit the other side.

Overload: “Bombarding” the opponent with hostile information or over-inform him in the preliminary phase of the conflict.

Division: Changing the opponent's mindset about his interests' orientation.

Suggestion: The one side gives information that influences the opponent in different internal and principal fields, such as legal or ideological fields.

Paralysis: Pose an imaginative threat that affects the opponent's vital interests.

Pacification: Acting in a way in order to reduce the opponent's alertness.

Pressure: Give information that affects opponent state’s population and make them feel that their government is unreliable.

Exhaustion: Coerce the opponent to make useless operations.

Deterrence: Make the opponent believe that he is the most active player in the conflict.

Under which circumstances, Russia uses hybrid threats?

According to some analysts, there are four circumstances under which a state participating in a conflict may apply hybrid strategy (Lanoszka, 2016, p. 176). The four circumstances above also reflect Russia's intentions and aim through its hybrid threats. The first one has geographical criteria. The state using hybrid tactics has local interests, and it is dominant in the region (Lanoszka, 2016, p. 176). In the first situation, global escalation dominance is not necessary because the belligerent probable wants to confine the conflict at a local level without any external intervention. Thus, in the case of Russia, it has greater military forces and can pose more significant threats to opponents that they expect to face.

The second situation has to do with the revision of a region's status quo or the expansion of a state's influence (Lanoszka, 2016, p. 176). Here, the use of hybrid strategy may be aiming to have as a result the rearrangement of opponent's borders and influence other state's regime politically — Russia, many times in the recent history, aimed at the abovementioned goals. The best example is the annexation of the Crimea Peninsula. However, the hybrid threat is more an aggressive strategy than a defensive one.

The third one has to do with the opponent's civil society and its population's diversity. The hybrid strategy can be ideal in a state which lacks civil society because of its composition; multicultural societies with ethnic, ideological or linguistic cleavages are more vulnerable to hybrid tactics because the belligerent state can influence these groups and destabilizes the regime from inside (Lanoszka, 2016, p. 176). Russia usually manipulates and influences such groups in order to serve Russia’s interests.

The fourth one is interconnected with the third. Some of these groups, usually minorities, have bonded with the belligerent state. These bond or common contact points give an informational advantage to the "hostile" state because it better understands the local competition or cleavages complaints (Lanoszka, 2016, p. 176). In Russian cases, Moscow tried to use the ties with the groups in order to find public legitimization for its actions within the borders of the opponent state.

Identifying Hybridity in Russia’s Actions

Having already analyzed in the first chapter of this essay the definition of hybrid threat and warfare it becomes easier to understand better the hybridity in Russia’s actions in some “conflict” situations between Russia and another state. Even though the essay concentrates on the hybrid threats, Russia poses in the Balkan peninsula, in the section we will make a more general analysis, taking into consideration multiple events and inter-state conflicts. Here there is also a question about whether Russia actually poses a hybrid threat and if its actions, in some situations, are legitimated. Furthermore, do Moscow's non-military means and techniques can serve its national interests? Is it a way to increase its influence in international affairs?

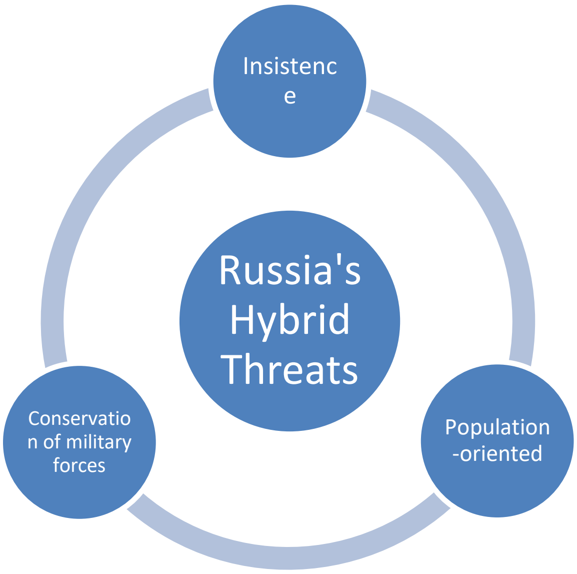
Some academics have already answered by categorizing the hybrid threat characteristics on Russia's actions. Christopher s. Chivvis distinguished three characteristics of hybrid threat. Based on his analysis Russia’s hybrid threats are the orientation of the actions to the population, the conservation on the use of force and its insistence (Chivvis, 2017, p. 2).

First of all, they have an orientation towards the population. After a meticulous observation, the last years, of the United States and their allies in crucial areas with great interest, (such as the Balkan Peninsula, the Middle East or elsewhere in the world) specialists and analysts on Russian external affairs and strategies, have come into a conclusion about the importance of influencing population of target states through operations using information, proxy groups and other functions or means of influence (Chivvis, 2017, p. 2). Russia uses the hybrid war within existing structures, political and social, aiming to carry out further Russian vital goals.

Moreover, Russia has conservation on the use of forces. In other words, Moscow seeks to serve its interests without using, as much as possible, military forces. As part of its overall hybrid strategy, we can include the use of conventional means or nuclear threats (Chivvis, 2017, p. 2). A good example is the use of electronic tools, cybersecurity threats or fake news. Although, the main point, in general, is that Russia wants to avoid using its traditional military forces.

Russia also distinguishes because of its insistence. The hybrid war disunites the traditional binary boundary demarcation between peace and war. The reality in this type of war imposes constant changes in conflict intensity (Chivvis, 2017, p. 2). Strategies in hybrid wars are always in progress, although they sometimes have to coexist or to cross-function with conventional warfare.

Table 2.3 Characteristics of Russian Hybrid Threats



Source for the data: (Chivvis, 2017, p. 2)

Russian Aims and Goals

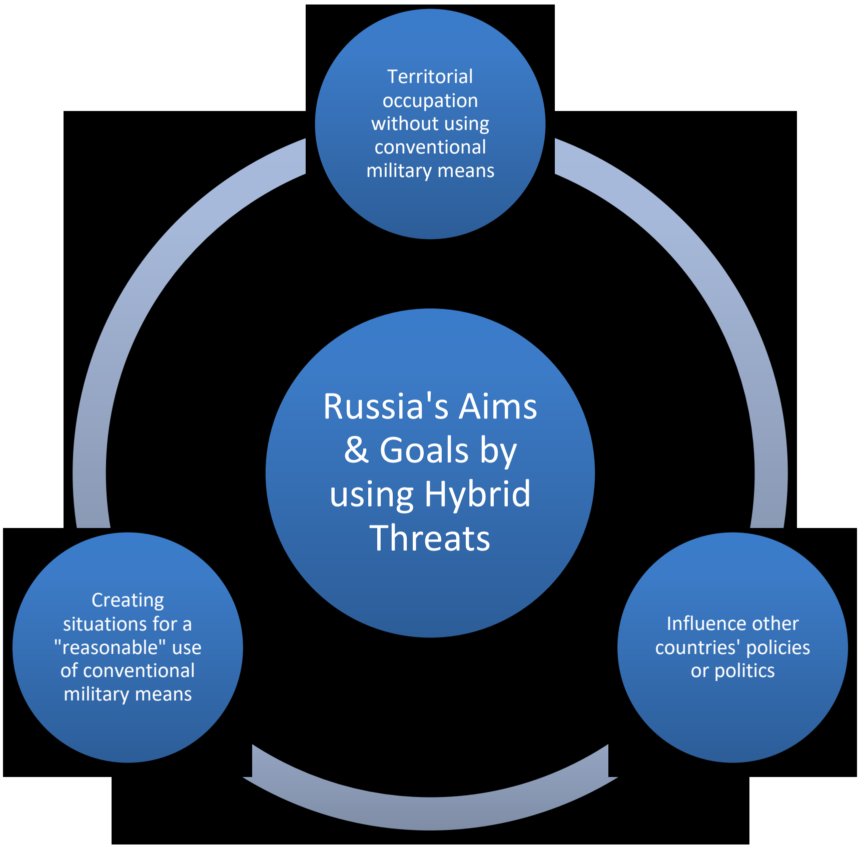
Nowadays, Russian application of hybrid threats seems to have some clear objectives. To start with, taking as an example Russia's annexation of Crimea, back in 2014, it seems that Russia proceeds to a territorial occupation without the appearance or the conventional use of military forces. Moreover, that was the key to Russia's success in our example and started the conversations about "hybrid strategy." This action supported by a Russian new-entry type of country's Special Forces, the famous "little green men" (Chivvis, 2017, p. 2). The use of this "tool"-part of the Russian military Special Forces, in combination with an information campaign on war and the development of reliable proxies on Russia, created the proper conditions for the bloodless annexation of Crimea.

The abovementioned case was not the first successful attempt of Russia to apply such tactics; in 2008 had used the same tactics in the invasion in Georgia. In both cases, this type of conflict, on behalf of Russia impeded Ukraine's, and Georgia's tries to approach Europe and integrate with its Western part. Moreover, as Mr. V. Gerasimov, Chief of General Staff of Russia stated that non-military actions are more familiar in modern era conflicts rather than the conventional means (Bartles, 2016, p. 34) (Gerasimov, 2013, p. 24).

A second objective, and maybe the most important and the most pressing challenge for Russia's opponents; do not have to do with military actions and the use of hybrid tactics is not a forerunner of conflict or warfare. Russia applies hybrid means in order to influence other countries, just about all over the world, both in policies and politics (Chivvis, 2017, p. 3). The main aim in this is targeted to specific countries, in order for Russia to achieve its national interests. These countries, in the majority of situations, are those who lack anticorruption and legal measures, or those who "accommodate" groups having the same interest with Russia or they are quite friendly to Russian politics. Although, even some developed countries, with strong political structures, are resistant to such tactics

The third objective for Russia is that uses hybrid threats as the main reason-guise in order to conclude to a conventional military action. To be more specific, after the annexation of Crimea international opinion turned into a scenario that Russia creates a climate of concern disoriented other countries, aiming to use conventional military forces in another region in the world, such as the Baltic countries or the Balkans (Chivvis, 2017, p. 3). Based on this scenario, Russia could manipulate Russian minority groups in countries such as Estonia to come in dispute with the local government. In a case that the rights of minorities intruded or be threatened, Russia can have an argument and a justification for potential intervention, in favor of these minority groups. Operations like these can be combined with cyber tools and actions that may reinforce the tensions or make the situation more complicated. Such events could inflame further conflict between Russia and the opponent county or even other actors of the international chessboard, such as NATO (Chivvis, 2017, p. 3). Furthermore, Russia would try to affect public opinion in the broader area in order to cozy up to the population for Russia's intervention. On this scenario, proxy groups or secret operations with agents would also be part of Russia's hybrid strategy.

Table 2.4 Russia's Aims and Goals by using Hybrid Threats


Territorial occupation without using conventional military means
Russia's Aims & Goals by using Hybrid Threats
Creating situations for a "reasonable" use of conventional military means
Influence other countries' policies or politics

Source for the data: (Chivvis, 2017, p. 3)

Russia's Means and Instruments for Hybrid Warfare

Having already analyzed some methods and instruments used in hybrid wars, in this section we will detect these tools in Russia's actions and hybrid strategy. The analysis below attempts to have a 360^{o} approach on Russia's toolkit in hybrid warfare, starting with popular tools, which are also used in conventional wars.

Russia has a substantial diplomatic history because of its participation in great conflicts as centuries passed by; from the World Wars to the Cold War and the collapse of the Soviet Union, Russia has developed diplomatic skills in order to survive and in some cases to dominate. As a result, Russia seems to use its traditional diplomacy for political influence or military deterrence (Chivvis, 2017, p. 4). The abovementioned has to do more with its nuclear military capabilities, but in all cases, we categorize diplomacy in Russia's hybrid threat tools.

Another outstanding way to influence other states, which also is used as a hybrid tool in Russia hybrid strategy, is the direct and indirect economic influence, as Russia has great energy advantage because of its natural gas supplies and pipelines (Chivvis, 2017, p. 4). An excellent example of direct economic influence is dated back in 2006 and 2009, when Russia discontinued the natural gas supplies in its neighboring country, Ukraine, in order to oblige the second one to agree on lower gas prices between the two countries. The most common indirect economic influence has to do with Russia offers for investments in pipeline infrastructures, in countries that depend on Russia's energy supplies, having as central aim to have a general influence in these countries.

The Russian hybrid strategy also includes secret operations and espionage; it uses briber, methods for coercion and other tactics to increase its influence in key-politicians for promoting through them its interests. In this context, the modernization of the army is included (Chivvis, 2017, p. 4). The interesting thing here is found on the individual units, as some people argue, Russia has; these units have the onus to penetrate in other states and manipulate or create hybrid war situations there (Chivvis, 2017, p. 4). It is believed that in 2016 Russia intelligence agents, part of its official military intelligence, plotted to sabotage Montenegro's integration in NATO by overthrowing country's government and attempting to assassinate country's prime minister (Farmer, 2017).

Another exciting instrument Russia uses in its hybrid strategy is the human factor in the shape of unofficial representatives or proxies. In the majority of times, these representatives are groups of "fans" that accept or agree with the country's objectives. One of the most famous groups, which acts as Russia's proxy, is the biker club "Night Wolves". The group is also named "Putin's Angels" because of its close ties with Vladimir Putin (Unian Information Agency, 2018) and some academics have characterized it as *paramilitary and propaganda arm* of Vladimir's regime (Snyder, 2018, p. 140) or a state-sponsored project, because of their ultra-national and anti-American orientation. The group provided substantial support, both logical and ideological, in the pro-Russian forces in the area of Crimea and the rebel groups in Donbas and included in Putin's hybrid strategy (Zabyelina, 2017, p. 3).

One of the most well-known tools of the Russian hybrid strategy is the operations of information and the country's strategic communication (Chivvis, 2017, p. 3). Russia has developed these skills and successfully uses them in order to create political narratives in other states, regions or continents. Its two most important channels of communication are the Sputnik and Russia Today (Aladente, 2018), but Russia uses also targeted program on television finances Europeans think-tanks for its interest promotion and inflames through Internet fake new, trolls and rumors, creating in this way a multichannel and multilevel communication. The main aim of these tools is to reshape the events, to create a new sense for the truth and to inform in the way that benefits Russia.

Russia has invested a lot in information infrastructure in order to dominate over Western countries in the Internet broadcasted news and generally in the Media. In most cases Russia does not target a specific country or conflict; it aims, through an opportunistically way, to confuse the public opinion and create a climate of distrust and discontent (Kofman & Rojansky, 2015, pp. 5-6). Although it disorients people form those ideas because it gives a sense of equality in free press right and adequacy in the given information; the motto used by Russia Today is "question more".

As we are in the cyber era, cyber tools are an integral part of the state's strategies, too. Also, of course, we include cyber tools in Russia's hybrid strategy (Chivvis, 2017, p. 3). Many people argue that Russia has "cyber warriors" who have developed skills and tools and intervene in other countries achieves, secret files and information systems. In the same context, in 2016 Russia has been accused of attempting influence US presidential campaign.

The Russian counterstrategy of a hybrid threat today

According to an article from the Russian journal "Military Thoughts," today's Russian counterstrategy concerning the concept of hybrid war can be both, offensive and defensive. Taking into consideration the constant changes in the political sphere, this outlook helps Russia to develop and implement its countermeasures against the opponent state, based on data taken from all levels of country's intelligence (Military Thought Journal, 2018).

Along with the central concept of hybrid war and its particular operation, the phase of the examination and the evaluation of a situation should include the extraction of information of hidden subversive elements. It is essential to understand, though, that these elements can also be found in isolated networks or groups throughout the country (Military Thought Journal, 2018). A useful method in this context applying in the central region is to create reconnaissance-strike groups that have their channels of communication; these group channels are usually more operation and reliable because of their secretive character. In this way, an independent source of information and an extensive intelligence network is created.

Based on the article some elements should also be taken into account (Military Thought Journal, 2018):

- Protest movements that are searching for sources of sustainable and then armed formations. These movements may use both external and internal capabilities.

- Identifying existing extremist social groups or political associations that are capable of participating firstly in planned non-violent actions and then in violent ones, including civil war situations.

- Identifying dangerous slogans or quotes that are as close as possible to the real demands of extremist social groups, whose actions ultimately can be used to undermine legitimacy or break the existing regime’s power.

- Suspicious preparation and training of groups to become leaders that may be capable of leading political protest movements, aiming a “coup d'état”.

- Commanders or fighters who are training in specialized camps or other military fields, preparing for military actions and organizing mobilization points and routes outside of the country in order to have a future possibility of transferring mercenaries.

- Person or group that support extremist elements in opposition to the regime and expanding into the borders of the central region; primarily through coordinated use of electronic-controlled domestic and foreign portals or other online media. Considerable attention is given if these groups gain the international community's support and international organizations', as well.

- To organize network structures for the management of subversion, supply, communication, and monitoring of a situation.

Russia's Targeted Areas

Analyzing Russia's hybrid warfare strategy, we can categorize countries targeted by Russia in three-tier groups (Chausovsky, 2017). In the first one, there are Russia's neighboring or closest countries such as Ukraine, Georgia or Moldova; states that traditionally depend on Russia economically or have a Soviet past and seem to be quite vulnerable in Russia's tactics and strategy. In these countries, Russia uses both conventional and non-conventional means, especially economic or energy cut-offs, as long as a socio-political influence.

The second tier country group includes more countries, also close to Russia but not neighboring (Chausovsky, 2017). These are the Balkan states, the Baltics and countries in Central and South Europe. In these countries, Russia could not use conventional means, because many of them are part of NATO and are protected. The hybrid strategy here includes cyber-attacks the use of ethnic Russian populations and also cut-offs on economic and energy fields. In the next chapter, we will analyze by cases hybrid threats posed by Russia in Balkan states.

Last but not least, the third tier group includes the core Western states such as the United States of America, France, and Germany (Chausovsky, 2017). In this group, Russia attempts to manipulate their political system, through disinformation tactics, fake news, trolls, propaganda and hacking attacks. The main Russian aim, through these actions in this tier, has as target the destabilization of these countries' and the debilitation of the Western unity within the gulfs of EU and NATO.

Chapter 3 Cases of Russia’s Hybrid Threats in the Balkans

Russia, as we have already mentioned, is targeting different groups of countries as for its hybrid warfare strategy. In this chapter, we are not going to elaborately analyze all Russian hybrid threats in different regions, but we are going to focus more on the Balkans and some events in neighboring countries of Eastern Europe. All these strategic movements aim to fulfill the vision of the President, Vladimir Putin, i.e. to make Russia a superpower again.

Furthermore, Russia's modern strategy concerning its intervention campaigns in other countries, prove that Russia has a different orientation than in the past. In the 21st century, and after the country’s intervention in the civil war of Syria, away from its traditional sphere of influence, Russia intends to expand its influence in a broader region (Bechev, Rival Power: Russia's Influence in Southesat Europe, 2017, p. 179).

Russia, having different ways to apply its hybrid strategy, uses much technology to impose security threats and influence all possible allies to have also implicit territorial presence. All these modern threats, with different tools, posed by Russia, make the country's "*force more visible now than at any point since the end of the Cold War”* (Bechev, Rival Power: Russia's Influence in Southesat Europe, 2017, p. 180).

In the Balkans, and generally in the southeastern part of Europe, both NATO and the EU attempt to have the dominant role in the region. Those two entities are Russia's competitors in the influence game, and countries try to find the best cooperation for their best interest, continually changing the power's equilibrium in the region (Bechev, Rival Power: Russia's Influence in Southesat Europe, 2017, p. 246)

As the ongoing economic crisis in the region has an effect on both NATO and the EU and as countries experience great readjustments and rearrangements in their internal field and policies, Russia finds appropriate opportunities and take the advantage in order to apply its influence and strategy (Bechev, Rival Power: Russia's Influence in Southesat Europe, 2017, pp. 17-19)

Russia’s influence in the Balkans: 21st century’s strategy

One of the main Russian focus areas is found in the Balkan Peninsula. Notably, the western Balkan area forms a core target in Russia's hybrid strategy in Europe. Of course, many reasons contributed to Russia’s concentration in this area; Balkan dissatisfaction with the region's progress in the European integration process, dissatisfaction related to the economic situation, ethnic pressures and cultural links with Russia, have made the Balkan Peninsula very attractive and ideal for Russia’s hybrid strategy.

CASE 1: Cyber Attacks against Montenegro and attempt of a coup

Montenegro is one of the most common targeted countries for Russia's hybrid strategy, and specifically for Russia’s cyber-attacks and espionage through the Internet. It is worth mentioning that these attacks have increased notably, after Montenegro’s application for membership in NATO. The concluded negotiations took place on May 2016, while the country became a NATO member in 2017. According to Montenegrin government statistics, the number of cyber-attacks has increased in just three years (from 2014 to 2017), from 22 attacks to 400. The most often targets were the Media and, of course, the country’s institutions (Tomovic & Zivanovic, Russia’s Fancy Bear Hacks its Way Into Montenegro, 2018).

As reported by the Montenegrin Ministry of Public Administration the situation was very severe for the country; there was an increased number of cyber-attacks in the state’s structures, phishing campaigns against public servants, many cases of cyber espionage and hacking cases also in the private sector, targeting banks and companies (Jonsson, 2018, p. 86).

On October 2016, Russia was accused of attempting a coup against the Montenegrin pro-NATO government (Higgins, 2016), an action which was in conjunction with large-scale Ddos attacks, on October 16th, during the parliamentary elections. Primary targets of these attacks were the government's sites, network infrastructures and websites of civil society, electoral monitors, pro-NATO parties and pro-EU political parties (Garcevic, 2017). Among the pro-governmental and state institution’s sites that got hacked during this mass cyber-attack, were the electoral observers “the Center for Democratic Transition”.

After these attacks, a big part of the Media blamed Russia for the events, with some of them arguing that hackers against Montenegro were the same as in US elections in the same year (Balkan Insight, 2017), as cyber security experts identified the attacks and the responsible hackers (Hacquebord, 2018). The detected hackers group, namely Advanced Persistent Threat 28(APT 28) directed by the Russian military intelligence agency. The same group had been accused of attacks also in German Media, in the French TV5 and US elections in 2016. Apart from the Media, the Montenegrin government also considered Russia responsible for the attacks and accused the country of stepping in the elections' process (Balkan Insight, 2017).

Regarding the abovementioned attempt for a coup, the Montenegrin police, the same day as the cyber-attacks, proceeded with suspects arrests. All in all, twenty people originated from Montenegro, Serbia, and Russia were arrested, as well. According to Garcevic testimony, Eduard Shirokov and Vladimir Popov, Russian intelligent agents, were the organizers of the coup. The main aim of this action was the prime minister's assassination (Garcevic, 2017). Both officers got arrested in Serbia, having in their possession uniforms of the Special Forces of Montenegro and prosecuted for the coup attempt along with other twelve people (Bechev, The 2016 Coup Attemt in Montenegro: Is Russia's Balkans Footprint Expanding?, 2018).

Another cyber-attack happened in January 2017 having as target Montenegro’s Ministry of Defense. The attack had the form of phishing, and the apparent senders were from NATO and the European Union. The main aim of the cyber-attack was to send emails with attachments, in order to install malware and steal sensitive data and private information in officer's computers. The malware was inside the attachment, and the responsible group was again APT28 (Paganini, 2017).

One month later, in February, governmental sites, state institutions and pro-governmental media got targeted again, through a much larger DDoS-attack campaign than the last one in the Election Day (Jonsson, 2018, p. 88). After the attacks the government of Montenegro observed that the intensity, the diversity and the professionalism of the cyber-attacks were the outcomes of synchronized cyber actions

(Balkan Insight, 2017); an investigation of three Montenegrin security companies argued that the attacks in February also came from the group APT28 (Tomovic & Zivanovic, Russia’s Fancy Bear Hacks its Way Into Montenegro, 2018). Despite all these cyber-attacks, Montenegro finally joined NATO in June, against Russia's interests, but fear for future Russian threats still exist in the country (Jonsson, 2018, p. 88).

CASE 2: Disinformation campaigns in Serbia and the role of Media

Russia also has great experience in guiding information and using the media for its own interests. Many Russian actors, such as research agencies, governmental sites, embassies, and civil society organizations, use the Media extensively for misinforming or for applying propaganda methods. According to a FYROM's intelligence report Russia's intelligence agencies seemed to be behind many journalistic activities of Russia, especially agents who work and live outside the Russian borders (Harding, Belford, & Cvetkovska, 2017).

Furthermore, one of Russia’s favorite countries in which apply such methods is Serbia and generally Serbian-speaking groups. According to the Serbian think tank “The Center for Euro-Atlantic Studies”, in May 2016, they found that there were active in Serbia over fifty pro-Russian organizations of both citizens and students’ associations (Center for Euro-Atlantic Studies, 2016, p. 82). This guided information polyphony blared the Medias’ transmissions and their credibility.

One the information satellites of Russia, was used in the country’s hybrid strategy concerning misinformation campaigns, is Sputnik Serbia. This channel of information is very crucial because it does not transmit information only in Serbia, but also in other areas of the Western Balkan region (Jonsson, 2018, p. 88). Another Russian governmental Media agency is Russia Beyond the Headlines (RBTH), owned by RT and part of TV Novosti. The Media became a more dangerous threat for Serbia after launching a pro-Russian mobile informational application in Serbia, FYROM, and Slovenia. The majority of the stories published or broadcasted by these Media often use Russophile rhetoric, which was many times Orthodox-oriented and of course against NATO and the EU. A characteristic example was the publicities from Montenegrin in a pro-Russian context promoting the military cooperation with Russia, giving at the same time notices to oppose the expansionism of the Albanians (Tomovic, Pro-Russian Montenegrins Publish New Anti-Western Media, 2017).

The content of the publicities accuse the Western countries of provoking upheavals in the broader region; revolutions such those in Georgia or Ukraine (Rose and Orange Revolutions, respectively) and attempts of overthrowing the leader of Republica Srpska in Bosnia, Miroslav Dodik (Jonsson, 2018, p. 89).

This part of Russia's strategy in Serbia can be characterized quite successful and productive as pro-Russia publicities and Russian narratives dominated in Serbian Media and opinion polls. Russia also achieved to establish its two original information channels, Sputnik Serbia and RBTH, in the region's daily newsfeed and its news to be republished every day, in information outlets in Serbia, Montenegro, and Bosnia (Cappello, 2017). Year after year the Russophile information agencies in Serbia showed a marked increase, with Sputnik being the most republished and quoted external source of information in the country (United States Senate on Foreign Relations, 2018, p. 82). It is worth mentioning that Sputnik supplies with news and generally information more than twenty radio stations in Serbia (Byrne, 2017).

Moreover, both Russian information agencies, RBTH and Sputnik, have a distinct advantage against other Media of the country because they are better organized; they have a constant and consistent newsfeed and have adapted better to the information demands of the new digital era in the Media industry (Jonsson, 2018, p. 89).

Another advantage, Sputnik has in contrast with other Media channels, is that it provides the possibility of repost and share with no charges; in this way, journalists and other channels of information can republish Sputnik's narratives promoting indirectly pro-Russia news and articles, which reflected in the majority of press agencies in Serbia (Jonsson, 2018, p. 89). Needless to say that Russian channels use a more attractive for the reader storytelling, following the click-bait trends on journalism.

According to Serbian opinion polls, Russia's strategy can be characterized more than successful within Serbia. To be more specific, 42% of Serbia's population finds Russia a reliable, supportive ally, in contrast with the 14% pro-EU voters (United States Senate on Foreign Relations, 2018, p. 81). Furthermore, despite the fact that in practice Serbia seems to be closer with NATO, based on its military-to-military exchanges with the Organization and in contrast with the Russian ones, according to opinion polls, 41% of Serbians voted against NATO, as they saw it as a threat (Jonsson, 2018, p. 90).

Additionally, concerning the investments within Serbia, the EU has provided and invested more in many areas than Russia, despite the population's beliefs for the exact opposite. It is important to mention that many countries in the region of Western Balkan Peninsula have the same sense, even if they are closer to the EU because of their integration in the Union and their economic and trade relations. Russia, through its hybrid strategy using disinformation campaigns, propaganda and strategic communication, has achieved to change the equilibrium regarding the region's strategic alignments. Moreover, as Russia’s popularity remains in high levels in the Balkan states, a growing distrust of the EU is being created, and this is the key of Russia’s hybrid strategy with misinformation tools success (European Parliament, 2017).

CASE 3: The Humanitarian Emergency Situation’s Center in Naftna Industrija Srbije

Observing Russia's strategy in Serbia, one very interesting point is its twofold position. Having already analyzed the misinformation campaigns we are going to see a different case of Russia's actions in Serbia. Also, we need to have in mind that countries as Serbia that do not have common borders with Russia, have a different opinion on Russia's threats.

In April 2012, in the southeastern Serbian city Nafta Industrijia Srbije (NIS), Russia created a Humanitarian Emergency Situation's Center in order to contribute in emergencies, such as natural disasters, operating relief activities and campaigns.

Examples of an emergency like this were the devastating floods that occurred in Bosnia and Herzegovina, in Serbia and Croatia. This was the official identity of the center (Bechev, Rival Power: Russia's Influence in Southesat Europe, 2017, p. 187).

However, there were many Media in Serbia arguing that the humanitarian identity of the center was a cover and that the final objectives of its actions were the creation of a Russian military base. This argument had its base on the issue that the co-finder entities of the center were *the Russian Ministry of Civil Defense, Emergency Situations and the Elimination of Consequences of Natural Disasters had a semi-militarized structure* (Bechev, Rival Power: Russia's Influence in Southesat Europe, 2017, p. 187). Furthermore, a year after the agreement, Mr. Sergei Shoigu became Minister of Defense; Sergei had initially signed the abovementioned agreement.

In addition, there were also those in Serbia and the United States, arguing that the the Center was a military outpost serving Russia's interest. These claims reinforced after Russia's demand to ensure center's personnel diplomatic immunity as well as the equivalent NATO's personnel. Russia, with this action, showed that for Moscow this center should be treated as equal to the Alliance (Bechev, Rival Power: Russia's Influence in Southesat Europe, 2017, p. 188).

CASE 4: Russia's Energy Strategy as Hybrid Tool in Bulgaria

One of the most potent tools Russia uses in the Balkan Peninsula, in order to serve its interests, is the energy sector. As the dominant energy supplier in the region, because of its oil and gas sources, and as many countries depend on Russia concerning energy, the country holds the advantage of using the sector as a promoting tool and a pressure point to expand its influence. Furthermore, the Russian companies play a crucial role in Russia's strategy, as though their investments and their commercial activity contribute to the reinforcement of Russia's supremacy in the region (Clark & Dr. Foxall, 2014, p. 7).

These companies play the role of Russia's satellite in the area that they are active; through their investments, Russia's position strengthens, as they achieve the creation of regional networks of economic interest and the reduce of generic competition in the energy sector. Those companies, both private and state-owned, have a significant presence in the energy market in the Balkan Peninsula, something that started in such an extent in the post-Soviet era, benefited by the privatizations occurred in Russia (Clark & Dr. Foxall, 2014, p. 7).

One of the Russian companies that also serve the country's interest is Gazprom. Part of the company's strategy in the Balkan Peninsula was to build the South Stream gas pipeline and to own the oil company Naftna Industrija Srbije (NIS) in Serbia. The idea was to construct a pipeline that will pass from Bulgaria to Austria through Serbia, Hungary, Slovenia, Croatia and Bosnia, and Herzegovina. After NIS's privatization in 2008, Gazprom took the majority stake of the company. This happened without a tender process and in exchange of a small fee, proportional to the size of the company, less than a fifth of its acquisition value (Filipovic, 2007). Apart from its activity in gas and oil supplies in Serbia, NIS also has almost four hundred petrol stations and one gas refinery in four Balkan countries (Bulgaria, Romania, Serbia, Bosnia, and Herzegovina).

Bulgaria is very dependent on Russia's energy resources, and Russia seems to have used the country, through the energy supplier companies, in order to extend its sphere of influence in the Balkans. An excellent example of this has to do with companies participated in the tender to construct South Stream's section in Bulgaria. The two companies were the Russian Stroytransgaz and the Bulgarian company Gasproekt Jug. After the annexation of Crimea in 2014, the United States put in the blacklist the Stroytransgaz and its owner with the accusation of Russophiles tensions and activities (Clark & Dr. Foxall, 2014, p. 8). That showed how Russia's influence is considered as a threat to other great powers not only in local but also in international level. In general, Bulgaria accommodates a large number of pro-Kremlin Russian companies, with considerable influence within the country through their high activity.

Russia's influence also appeared in Bulgaria's decision, in 2012, to cancel the license of exploration gas reserves, from the American-interest energy company, Chevron. This decision was, apparently, the result of protestors' pressures that were supported by the Russian government. Furthermore, Bulgaria's policy seems to also being influenced by business networks and companies with Russian economic support or other ways of influence and dependence. (Chivvis, 2017, p. 4). Not only Bulgaria's decision makers but also the citizens seemed to be influenced by Russia; in 2014 there were suspicions that anti-shale gas and other Bulgarian protesting groups and movements supported by Russia. The anti-shale gas movements have hindered Bulgarian efforts to eliminate energy dependence on Russia (Hope, 2014).

CASE 5: Bosnia & Herzegovina: Republika Srpska cooperates with Russia

Another target country in Russia’s hybrid strategy is Bosnia and Herzegovina. This country seemed vulnerable to Russia's influence, especially for the aim of the country's destabilization a few months before its elections in October 2018. This vulnerability has its roots in the country's composition with two decentralized structures. The one is Bosnia's and Herzegovina's Federation, consisting of Croats and Bosnians in the majority and the second one is the Republika Srpska, mainly consisting of Serbs. In a situation like the abovementioned, Russia’s hybrid strategy aims to reinforce and maintain Republika Srpska’s separatist tendencies (Mironova & Zawadewicz, 2018).

Back in 2016, a Russian delegation in an official visit in the headquarters of Republika Srpska in Banja Luka, discussed the establishment of cooperation between the police of the two governments, in the field of intelligence, fighting against cybercrime and counterterrorism. The two sides agreed to exchange their units, for training and educational purposes (especially from the Republika Srpska special Serbian are sent to Russia), as long as for work (Mironova & Zawadewicz, 2018). It often occurred between the two governments to share the military knowledge and to have interpersonal social relations among their security personnel. The members of Republika Srpska also have Russophile views; a former officer of the government’s intelligence agency, Predrag Ceranic, in his book with the title “*Who Gets Bothered by Little Russians”,* with this characterization is referring to Serbians.

Furthermore, there were discussions between the two entities in order to create Russian Humanitarian Center that will have as main aim to help Republika Srpska in case of natural disasters. The same center has also been established in Naftna Industrija Srbije (NIS) in Serbia, where Russia has asked for its personnel diplomatic immunity. In addition, the two entities have created strong bonds between their organization's members, which are war veterans. These organizations have participated with private military companies originating from Russia, as foreign fighters in conflicts in Syria and Ukraine. Moreover, the veteran’s organization from Banja Luka is also associated with a paramilitary organization from Serbia, whose members have also been trained by the Russian military (Mironova & Zawadewicz, 2018). Last but not least, when Republika Srpska decided and announced the establishment of a training center in an area close to Banja Luka, Russia suggested providing in the center, military forces from Serbia specializing in anti-terrorism techniques, aiming to strengthen the center by creating counterterrorism units and department for fighting against organized crime.

Conclusions

Hybrid threats are not a new-entry term in international relations. There are many definitions for the term and different ways to categorize each situation with hybrid characteristics. Furthermore, there is also a gradation of the term; from the hybrid threat to hybrid conflict and warfare, with almost the same characteristics but they reflect a sharp escalation of a conflict, in which the tactics are applied. Additionally, hybrid threats seem to have similar characteristics with other threats as the asymmetric ones, but always there is a line with characteristics that differentiate them. As with threats, the same thing happens with hybrid warfare; there are differences between the term, the irregular, and conventional warfare.

In the 21st century, hybrid strategies have become very popular. States try to achieve their goals by using non-conventional means, without using military forces. The most interesting in this is that those hybrid strategies, so far, have been proved very effective as in the majority of the occasions, the state who applies such strategy actually succeeds, without being noticed from the rest of the world.

In the second chapter, we generally analyzed the hybrid strategy of Russia. Its past, Soviet techniques such as *Maskirovka* seem to have incorporated into its modern hybrid strategy. The two most potent instruments in Russia's toolkit are the manipulation of information and cyber warfare. Both alternatives to hybrid strategy are more topical than ever, as they are contemporary and they are in line with technological developments and the needs of the modern world. Three significant characteristics that we observed in Russia's hybrid threats are the conservation of military forces, the population-oriented strategy because the population seems to be the most vulnerable element in a targeted society and its insistence no matter what the outcome of the strategy is.

In the modern era, Russia's attempts to expand its sphere of influence are very obvious, especially in Southeastern Europe. Apart from its hybrid strategy applied by the government, Russia also has as a powerful tool of pressure, its gas and oil reserves, in cooperation with the Russian energy production companies. The cases described in the third chapter proved that Russia has many different ways to serve its private interests. Moreover, it seems that these interests are expanded in the broader area of the southeastern part of Europe and the most vulnerable countries of Russia's hybrid strategies are its neighbors and the Balkan states.

Another important thing is that Russia not only targets countries in order to spread its influence in the internal of these states but also in order to be more potent in them in comparison with the EU and the NATO. In other words, Russia has vital interests generally in the region and has two aims in order to achieve; firstly to have an effect directly in the vulnerable states and those who can easily be influenced by Russia and secondly to dominate indirectly over EU and NATO sovereignty.

Based on the abovementioned analysis, we can come to the following conclusions. To start with, hybrid threats and generally the hybrid strategy is something that has its basis from the ancient world. Through the centuries and because of the advance of technology changed a little but the idea remained the same; the effort to serve a state's or a group's or a side's interests, by damaging the opponent, without using direct military forces and sometimes in a way that the other side would not even understand it.

Moreover, Russia has been an active player in the region. As Dimitar Bechev wrote: "*the Kremlin is pulling all the strings in this game".* (Bechev, Rival Power: Russia's Influence in Southesat Europe, 2017, p. 248). Moreover, it seems to be right if we observe the country's strategy and its goals. Many other players support Russia's actions in the background, such as private companies, organizations, other countries' leaders or organized population groups. Although the West also seems to become a more energetic player in the international chessboard regarding the hybrid strategy; not only against Russia's aims but also in favor of their interests. This is only the start of the "old-new" way states claim what they want, and hybrid strategies have a long way of evolution.

Until now, we observe that Russia increasingly prefers the use of such strategies, but are they actually successful in the Balkans? It depends on the perspective; Russia's individual actions seem very successful as the country exerts its power and influence against others, but if our premise is how other states are detached to EU and NATO then we can argue that the strategy is not as effective as it seems.

And this is the reason so far Russia is not a threat for the regional stability and security. However, other actors have already done some strategic movements in order to prevent a future scenario like this; in 2015 NATO announced the establishment of a new Hybrid Warfare Strategy. Having in mind Russia's development rate and its aims and goals, it seems that we are in the threshold of a new era, where Russia is not West’s biggest threat yet and in the near future, maybe, there will be a greater need to confront Russia’s advanced hybrid strategies.

To sum up, we do not know yet if Russia is going to become a superpower again in the international arena. Although we can say, as it seems, that is a solid player regarding hybrid strategies and in achieving its regional goals; this is also reflected in its internal interests. Russia’s strategy is basically hybrid in the 21st century and as years go by it seems to exploit it in larger extent. And as the model of hybrid warfare becomes mainstream, in the next years, we are going to observe more and more alternative ways of application of such strategies, and maybe the majority of conflicts will be conducted in this way.

Bibliography

Aladente, D. (2018, January 2). *El Pais*. Retrieved December 28, 2018, from El Pais: https://elpais.com/elpais/2018/01/02/inenglish/1514887171_124173.html

Andersen, B. W. (2012). Clausewitz's Continued Relevance and Foundation for Educating Critical Thinking Skills. *U.S. Army War College Carlistle Barrack*, 1-36.

Arquilla, J. (2011). *Isurgents, Raiders, and Bandits: how masters of irregular warfare have shaped our world.* Chicago: Ivan R. Dee.

Balkan Insight. (2017, January 10). *Montenegro on Alert Over Rise in Cyber Attacks*. Retrieved January 18, 2019, from Balkan Insight: http://www.balkaninsight.com/en/article/montenegro-on-alert-over-cyber-attacks-01-09-2017

Bartles, C. K. (2016). *Getting Gerasimov Right.* Military Review.

Bechev, D. (2017). *Rival Power: Russia's Influence in Southesat Europe.* Yale University Press publications.

Bechev, D. (2018, April 12). *Foreign Policy Research Institute*. Retrieved January 18, 2019, from Foreign Policy Research Institute: https://www.fpri.org/article/2018/04/the-2016-coup-attempt-in-montenegro-is-russias-balkans-footprint-expanding/

Berzins, J. (2014, April). Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Forces. *National Defence Academy of Latvia Center for Security and Strategic Research*, pp. 1-14.

Binnendijk, H. (1998). Assymetric Threats. In H. Binnendijk, *Strategic Assesment: Engaging Power for Peace* (pp. 169-184). Washington: National Defense University. Institute for National Strategic Studies.

Brauch, H. G. (2011). Concepts of Security Threats, Challenges, Vulnerabilities and Risks. In H. Günter, Ú. Brauch , S. Oswald , M. Czeslaw , J. Grin, P. Kameri-Mbote, . . . J. Birkmann (Eds.), *Coping with Global Environmental Change, Disasters and Security:Threats, Challenges, Vulnerabilities and Risks* (pp. 61-106). Springer-Verlag Berlin Heidelberg .

Byrne, A. (2017, March 19). *Financial Times.* Retrieved January 19, 2019, from Financial Times: https://www.ft.com/content/3d52cb64-0967-11e7-97d1-5e720a26771b

Cappello, J. (2017, February 1). *Defense.* Retrieved January 19, 2019, from Real Clear Defense: https://www.realcleardefense.com/articles/2017/02/02/russian_information_operations_in_the_western_balkans_110732.html

Center for Euro-Atlantic Studies. (2016). *Eyes Wide Shut: Strengthening of Russian Soft Power in Serbia:Goals, Instruments and Effects.* Rockfeller Brothers Fund. Retrieved Jauary 19, 2019, from https://www.ceas-serbia.org/images/publikacije/CEAS_Studija_-_%C5%A0irom_zatvorenih_o%C4%8Diju__ENG.pdf

Chausovsky, E. (2017, August 9). Russia's Hybrid Warfare Strategy.

Chivvis, C. S. (2017). Understanding Russian Hybrid Warefare and What Can be Done About It. *The RAND Corporation*.

Clark, D., & Dr. Foxall, A. (2014). Russia's Role in the Balkans - Cuase for Concern? *The Henry Jackson Society*, 1-21.

Clausewitz, C. (1984). *On War.* (M. Howard, P. Paret, Eds., M. Howard, & P. Paret, Trans.) New Jersey: Princeton University Press.

Countering hybrid threats: EU and the Western Balkans case, PE603.851 (Workshop September 2018).

European External Action Service (EEAS). (2015, May 13). *Council of the European Union.* Retrieved Novemeber 18, 2018, from Council of the European Union:

http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf

European Parliament. (2017, July 6). *European Parliament.* Retrieved November 20, 2018, from European Parliament: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2017)608627

Farmer, B. (2017, February 19). *The Telegraph*. Retrieved December 28, 2018, from The Telegraph: https://www.telegraph.co.uk/news/2017/02/18/russias-deadly-plot-overthrow-montenegros-government-assassinating/

Filipovic, G. (2007, December 28). *Minister slams Russian grab for Serb oil monopoly*. Retrieved January 20, 2019, from Reuters: https://www.reuters.com/article/us-serbia-russia-nis/minister-slams-russian-grab-for-serb-oil-monopoly-idUSL2852531920071228

Garcevic, V. (2017, June 28). *Russian Interfirence in European Elections: Russia and Montenegro.* Retrieved January 18, 2019, from US Senate Committee on Intelligence: https://www.intelligence.senate.gov/sites/default/files/documents/sfr-vgarcevic-062817b.pdf

Gashi, B., & Maqedonci , E. (2017). The concept of hybrid threats and the challenges of modern times. *20*(39/40), 91-102.

Gerasimov, V. (2013, February 26). The Value of Science is in the Foresight. *Voyenno-Promyshlennyy Kurier*, 23-29.

Hacquebord, F. (2018, January 12). *Targeted Attacks*. Retrieved January 18, 2019, from Trend Micro Security Intelligence Blog: https://blog.trendmicro.com/trendlabs-security-intelligence/update-pawn-storm-new-targets-politically-motivated-campaigns/

Harding, L., Belford, A., & Cvetkovska, S. (2017, June 4). Russia actively stoking discord in Macedonia since 2008, intel files say. Retrieved January 19, 2019, from https://www.theguardian.com/world/2017/jun/04/russia-actively-stoking-discord-in-macedonia-since-2008-intel-files-say-leak-kremlin-balkan-nato-west-influence

Higgins, A. (2016, November 26). *Finger Pointed at Russians in Alleged Coup Plot in Montenegro.* Retrieved January 18, 2019, from New York Times: https://www.nytimes.com/2016/11/26/world/europe/finger-pointed-at-russians-in-alleged-coup-plot-in-montenegro.html

Hoffman, F. (2014, July 28). *On Not-So-New Warefare: Political Warefare vs. Hybrid Threats.* Retrieved 11 5, 2018, from War on the Rocks: https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/

Hope, K. (2014, November 30). *Bulgarians see Russian hand in anti-shale protests*. Retrieved January 20, 2019, from Financial Times: https://www.ft.com/content/e011d3f6-6507-11e4-ab2d-00144feabdc0

Jonsson, O. (2018). The next front: the Western Balkans. In N. Popescu, & S. Secrieru (Eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies* (pp. 85-91). Paris: European Union Institute of Security Studies.

Kasapoglu, C. (2015). *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control.* Rome: NATO Defense College.

Kofman, M., & Rojansky, M. (2015, April). A closer look at Russia's Hybrid War. *Wilson Center*.

Lanoszka, A. (2016, January). Russia's Hybrid warfare and extended deterrence in eastern Europe. *International Affairs, 92*(1), 175-195.

Mansoor, P. R. (2012). Hybrid Warfare in History. In W. Murray, W. Murray, & P. R. Mansoor (Eds.), *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (pp. 1-10). Cambridge: Cambridge University Press.

Merriam-Webster (n.d.). (n.d.). Retrieved 12 2, 2018, from Merriam-Webster: https://www.merriam-webster.com/dictionary/hybrid

Merriam-Webster (n.d.). (n.d.). Retrieved 12 2, 2018, from Merriam-Webster: https://www.merriam-webster.com/dictionary/warfare

Miklaucic, M. (2011, September 11). *NATO*. Retrieved from NATO: https://www.act.nato.int/nato-countering-the-hybrid-threat

Military Thought Journal. (2018). Hybrid War Strategy and Counterstrategies. *Military Thought Journal*. Retrieved from http://vm.milportal.ru/strategiya-i-kontrstrategiya-gibridnoj-vojny/

Mironova, V., & Zawadewicz, B. (2018, August 8). *Putin Is Building a Bosnian Paramilitary Force*. Retrieved January 21, 2019, from Foreign Policy: https://foreignpolicy.com/2018/08/08/putin-is-building-a-bosnian-paramilitary-force/

North Atlantic Treaty Organization. (2010, August 25). *North Atlantic Treaty Organization.* Retrieved November 15, 2018, from North Atlantic Treaty Organization: http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

North Atlantic Treaty Organization. (2018, July 11-12). *North Atlantic Treaty Organization.* Retrieved November 15, 2018, from North Atlantic Treaty Organization: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180718_180711-summit-guide-brussels.pdf

Paganini, P. (2017, June 7). Russia-linked hacker group APT28 continues to target Montenegro. Retrieved January 19, 2019, from https://securityaffairs.co/wordpress/59820/apt/apt28-targets-montenegro.html

Pawlak , P. (2015). *Understanding Hybrid Threats.* European Parliamentary Research Service. European Parliament. Retrieved from https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/

Reyeg, F. M., & Marsh, N. B. (2011). The Filipino way of war: irregular warfare through the centuries. *Master Thesis Naval Postgraduate School*.

Rid, T. (2012). War will not take place. *Journal of Strategic Studies, 35*(1), 5-32.

Sari, A. (2017, March 5). Hybrid Warfare, Law and the Fulda Gap. *University of Exter, Law School*, p. 9.

Schleifer, R. (2006). Psychological Operations: A New Variation on an Age Old Art: Hezbollah versus Israel. *Studies in Conflict and Terrorism, 29*, 1-19.

Schuurman, B. (2010). Clausewitz and the "New Wars" . *Parameters, 40*(1), 89-100.

Snyder, T. D. (2018). *The Road to Unfreedom: Russia, Europe, America.* USA: Crown Publishing Group.

Thomas, T. L. (2004). Russia's Reflexive Control Theory and the Military. *Journal of Slavic Military Studies, 17,* 237-256.

Tomovic, D. (2017, October 18). *Balkan Insight.* Retrieved January 19, 2019, from Balkan Insight: http://www.balkaninsight.com/en/article/pro-russian-montenegrins-publish-new-anti-western-media-10-17-2017

Tomovic, D., & Zivanovic, M. (2018, March 5). *Russia's Fancy Bear Hacks its Way Into Montenegro.* Retrieved January 18, 2019, from Balkan Insight: http://www.balkaninsight.com/en/article/russia-s-fancy-bear-hacks-its-way-into-montenegro-03-01-2018

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). *Addressing Hybrid Threats.* Bromma: Swedish Defense University.

Unian Information Agency. (2018, July 26). Retrieved December 28, 2018, from Unian Information Agency: https://www.unian.info/world/10202310-putin-s-biker-gang-sets-up-military-style-camp-on-nato-soil-media.html

United States Senate on Foreign Relations. (2018, January 10). *US Foreign Senate.* Retrieved January 19, 2019, from US Foreign Senate: https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

Wilkie, R. (2009). Hybrid Warfare: something old, not something new. *Air and Space Power Journal, 23*(4), 13-17.

Zabyelina, Y. (2017, June 9). Russia’s Night Wolves Motorcycle Club: from 1%ers to political activists. *Trends Organ Crim* , 1-13.