Journal of Criminology and Forensic Studies
ISSN: 2640-6578

Academic Strive
Researcher's perception is our reality

Review Article *Volume 5 Issue 1*

Hybrid Threats, Challenges, and Dangers in Kosovo

Bucaj E[1] and Haziri F[2]*

[1]Public University "Ukshin Hoti" Prizren, Kosovo

[2]Faculty of Public Safety, Kosovo Academy for Public Safety and UBT College, Kosovo

***Corresponding author:** Fatos Haziri, Faculty of Public Safety, Kosovo Academy for Public Safety and UBT College, Fan Noli number 34, Prishtina, Kosovo, Tel: +38344506096; Email: facts.haziri@kosovopolice.com

Received Date: March 07, 2023; **Published Date:** April 17, 2023

Abstract

Fighting as a social phenomenon evaluates and changes continuously. While the term "hybrid war" has become a key element in the security vocabulary of the Western Balkans and beyond. At the same time, with the recent developments in technology, security organizations/ institutions are interested in increasing their preparedness for possible future wars. Because of the way of how currently security organizations/institutions are operating, there are reasonable concerns to believe that they cannot appropriately respond to new wars if it is approached in the same way as it has been done in the past.

In the absolute meaning of technological growth, the security institutions are confronting a change of perspectives and the preparation of a new social and cultural generation about how war will be understood in the future and the change of its shape at a time when it also changes the term "classical war." The term "hybrid war" is entering the security doctrine increasingly every day and is becoming an influential part. The threats that come from the hybrid war include propaganda, the creation of various misinformation expressed as fake news known as counterfeit information arranged, processed, and directed specifically to misinform, known as' deep fake'; cyber-attacks, intrusions into computer systems, various economic pressures; sabotage, financing the media, multiple portals; and well-known analysts of particular topics, mainly political security, economic issues, etc. The threats of hybrid war, in recent years, are felt to a large extent in the Western Balkans, so the security institutions have started to treat these issues seriously, and have undertaken various actions to prevent them. Such threats are felt in Kosovo as well. Due to its internal circumstances, regional context, and international developments, Kosovo is a country that can very quickly be exposed to hybrid threats.

Keywords: Kosovo; Hybrid Threats; Conflict; Durability; Prevention; International Cooperation

Introduction

The states of the Western Balkans have now experienced direct intervention by external factors through various methods of hybrid threats, where the primary focus is given to the creation of false information. These threats were combined with multiple cyber-attacks and direct terrorist acts, such as the example in Montenegro.

Russia and the USA have two completely different approaches to the Western Balkans. Russia tries to confuse the public and slow down the progress of the Western Balkans and its integration into Euro-Atlantic processes. At the same time, the USA offers support for building democratic institutions and their integration into such processes. Russian hybrid threats in the Western Balkans are occurring in different forms, such as cyber-attacks, propaganda, and the collapse of democratic processes. In most cases, hybrid threats are not easily detected, and even when they are detected, it is often too late to react as the damages that they have caused are usually irreparable. The recent developments in the field of information technology and its impact on society have created a suitable environment for the threats from the hybrid war which can start without previously having a conventional war, since hybrid warfare can be developed even in conditions of peace through the financing of propaganda media and the extension of controls, economic, sabotage of different levels, interventions in cultural and religious issues, interference in elections to influence the determination of the winner, etc.

The Western Balkans remain unstable, with an environment suitable for extending the influence of different countries through hybrid warfare with non-conventional methods. In the Western Balkans, threats from the hybrid war have increased in recent years, while NATO and the security institutions of respective democratic countries have started various actions to prevent them. Hybrid warfare is a threat to both large and small countries, including Kosovo. Fortunately, the conventional war has ended, but a combined hybrid war is taking place, influenced by external and internal actors. More than other countries in the region, Kosovo is exposed to hybrid risks due to the crisis and political polarization, the lack of sovereign security institutions, the fragile economic situation, the rule of law, and public safety. At the regional level, Serbia is always problematic regarding Kosovo due to its proximity to Russia. At the international level, the complete lack of recognition of independence and remaining outside of many international security organizations are prerequisites that may undermine Kosovo's security.

The Main Challenges in Western Balkans

Hybrid warfare is a military strategy that combines tactics of political warfare, conventional warfare, irregular warfare, and cyberwarfare with other methods of influence, such as "fake news ", diplomacy, lawfare, and external electoral intervention [1]. By combining field operations with subversive efforts, the aggressor intends to avoid accountability or retaliation [2]. The term Hybrid War can be used to describe the complex and flexible dynamics of the battle space, with a highly adaptable and resilient response [3].

"Hybrid war" is defined by analyst and author Frank Hoffman as a "blend of the lethality of state conflict with the fanatical and protracted fervor of irregular war [4]." The expanded definition is as follows:

Sophisticated campaigns combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perception and international opinion [5].

The move from Color Revolutions to Unconventional Wars is projected to dominate the destabilizing tendencies of the future decades, and Hybrid War is one of the most important strategic breakthroughs that the US has ever pushed. Those unfamiliar with viewing geopolitics through the lens of the Hybrid War may struggle to predict where the next one will occur, but it's really not that difficult to identify the areas and nations most vulnerable to this new type of aggression [6]. The key to the prediction is to understand that Hybrid Wars are externally triggered asymmetrical battles based on destroying specific geo-economic interests, and then go from there to predict where they would strike next.

The challenges of hybrid warfare in Western Balkan have grown to such proportions in recent years that even major governments and military organizations have begun to handle these concerns with the utmost seriousness, launching a variety of measures and training programs for military and civilian employees to combat them. The difficulty is that hybrid threats are not readily identified in most circumstances, and even when they are, it is typically too late to respond the harm done is generally irreversible.

These concerns, in particular, have been heightened by recent technological advances, particularly the global reach of social networks and their effect on the general public. The Western Balkans, as terrain and an unstable area, provide an ideal setting for the formation of such a conflict, in which, in addition to traditional techniques of combat, non-conventional and hybrid tactics of warfare are used. There are several instances on the ground in the Balkans, where regular and irregular armed forces have often been utilized.

We may argue that the danger of hybrid conflict in Western Balkan has grown to such a degree in recent years that governments and military organizations have begun with increasing of mutual cooperation in order to successfully address those threats. In most cases, the hybrid threats are not easy to discover, and even when they are detected, it is typically too late to appropriately respond to them.

Russian influence on Serbia and the contestation of many democratic processes in the Balkans as well Serbia's contestation of Kosovo's statehood, the particular hybrid war that Serbia conducts on a daily basis with Russia's help, influencing the economy, and unprincipled collaboration are significant challenges for Kosovo to overcome in the absence of strong international support. Following NATO's involvement and the declaration of Kosovo's independence, Serbia attempted to influence the economy via commerce through a hybrid war. Furthermore, the Special Court's accusations and prosecution of KLA members, as well as the formation of this court solely for crimes committed against Serbs, are part of a hybrid war waged by the Serbian intelligence service in collaboration with state mechanisms, various propaganda, and external actors, through whom the formation and installation of this court were initiated.

Even major governments, but particularly tiny small ones like Kosovo, might fall victim to this hybrid warfare; therefore, security agencies must consider the risks, risk assessments, and repercussions that these threats can bring. Many such examples can be found in the Balkans, such as the case of Macedonia, where a coup was attempted through various elements of unconventional warfare, propaganda from within and outside the state, and, ultimately, the use of violence, so that Macedonia would not be heading towards NATO membership at the time. Macedonia was not at war and had not declared one, but a mixed hybrid war was being built and influenced by foreign and internal forces. A database including the wages of hundreds of thousands of workers (including intelligence officers) was released in Albania a few months ago, and it is believed that the database was purchased by a team member of a Russian tycoon related to Putin.

The main challenge in the Western Balkans is the creation of mutual trust and unconditional cooperation in the exchange of cooperation information between law enforcement institutions in preventing and fighting the hybrid war, which so far has only one threat, Russia.

Russia's Hybrid Warfare in the Western Balkans

Russia intends to escalate the conflict in the Western Balkans, first via a successful hybrid war, in order to maintain disruptive measures and divert Western attention away from Ukraine and their efforts in the post-Soviet zone. The former Yugoslavia has emerged as the Kremlin's second battleground, with authorities stating that expanding the EU into the Western Balkans, whose states are less rich and troubled by both internal and regional difficulties, will weaken the community. As a consequence, Moscow cultivates a tight circle of sympathizers inside the European Union, and each failure of EU and NATO expansion in the Balkans is instantly promoted as a Russian propaganda weapon. Following Putin's consolidation of power, and especially after Russia's military involvement in Georgia in 2008, it has become clear that Russia is aiming to undermine Western democracies and incite anti-NATO and anti-EU sentiments.

Although the Western Balkans region is less important to Russia than the post-Soviet space or the "near abroad", Russia has been waging a "hybrid war" in the Western Balkans for two decades. In this "war", Russia managed to achieve considerable success (mainly in Serbia, and through Serbia in Republika Srpska, one of the two entities of Bosnia-Herzegovina), but also faced defeats (in North Macedonia and Montenegro) [7]. The pinnacle of Russian success is its dominance in the fuel and gas sector of Serbia and Republika Srpska [8]. Russia's foreign policy has been characterized by hostility to NATO expansion since the fall of the Soviet Union. This 2008 concept advocates opposition to future NATO expansion, notably the entrance of Ukraine and Georgia to NATO. In its Military Doctrine, authorized in 2010, Russia identified NATO expansion as the primary "external military risk," i.e. a threat to its national security. The term hybrid warfare has traveled, from being an irregular actor disposing of relatively advanced weapons to a regular actor pretending to be an irregular actor. It is important to understand that the term is a theoretical term and not an empirical one.

The West, i.e. NATO and the EU - is under constant attack today, this along with attacks on the international systems which is undermined by the inactivity of the West. Hybrid warfare has gone from being a description of irregular actors disposing of systems (primarily weapon systems) which one usually argues that states solely possess. The mass availability of high technological innovations, with the globalized economy, has been discussed as a possible new hybrid threat. Then, with the Russian annexation of Crimea and the war in Ukraine, the focus of the term once again shifted in another direction. Now the focus was more subtle, aiming at Russian deniability, reflexive control and what that could mean when it comes to the credibility of NATO and the EU. Organizations which to some extent can be expected to stand up for the international system of law and order. Espionage and network intrusion has preceded conventional military invasion, providing a warning before the conflict escalates to the use of force. In the cases of the 2008 invasion of Georgia, and in Ukraine, Russian forces spent up to years monitoring governmental networks. Any evidence of Russian intrusion serves as something of a warning shot – a very long one. Russia executes its control over its territory in a manner that adds to the multifaceted nature of hybrid warfare. Not only does the international community need to deal with the variety of operations occurring inside and outside of cyberspace, but it also has to examine the relationship of a wide variety of groups and organizations in determining liability.

If there had been a response to aggressive behavior within the Ukrainian network sphere, perhaps the West could have had a more expedient and cohesive response to the Russian physical invasion. The kinds of operations that Russia is conducting in Ukraine are not terribly novel, or even that sophisticated; rather, they exploit the fact that any operations in the cyber domain are befuddling Western nations. The Russian Federation has as a creed Lenin's idea that „If Russia cannot control a country, then that country has to be at least destabilized [9]".

Hybrid Challenges in Kosovo

In recent years, the West has begun to face new security threats which, due to their non-conventional nature, are being described as hybrid threats. Kosovo is a country that can very easily be exposed to hybrid threats due to internal circumstances, regional context, and international developments. In essence, hybrid risks are being undertaken by state and non-state actors. Hybrid threats represent the newest form of confrontation between the West, Russia, and other countries. Another hybrid threat is the ongoing interference of unfriendly international countries to influence the public image of the government and influence the political orientation of the current government and other governments. Kosovo is also exposed to cyber-attacks which can highlight the secrets of politicians, blackmail that can happen against the state and public interest of Kosovo, the instigation of political conflicts, and change of the political regime not dictated by the democratic will of the citizens. and constitutional rules, but from external interests, as happened in the case of Macedonia, I can damage the critical infrastructure of public and financial institutions, as well as I can damage the general functioning of the state. Although Kosovo enjoys a very young population where the average age is 25.9 years [10], 70% of the population is under 30 years old, while 33% belong to the 0-14 age group and only 6% are over 65 years old [11] and IT users are mainly young people where 98.8% of the population use the Internet every day [12] cybercrimes and hybrid attacks through computer technology have not increased compared to other countries.

	Number of incidents
2019	
327* Intrusion into computer systems	89
336* Identity theft and access device	13
339 Intrusion into computer systems	71
2020	
327* Intrusion into computer systems	180
336* Identity theft and access device	35
2021	
327* Intrusion into computer systems	189
336* Identity theft and access device	19

Table 1: Annual statistics.

The term hybrid warfare is increasingly being incorporated into security doctrine and is becoming an effective part of the long-term and annual plans of all law enforcement agencies. The threats deriving from the hybrid war include propaganda, the deliberate creation of various disinformation spread via fake news known as arranged fake news, which is processed and cracked in order to misinform the public and is known as 'deep fake', cyber-attacks, intrusions into computer systems, the various economic pressures, sabotage, financing of the media, various portals and opinion leaders known as analysts of certain topics, mainly political and economic, health, educational topics in one word "all-knowing opinion leader" who at the time of my prime 20:00-22:30hrs on almost seven national televisions are distributed with the sole purpose of disinforming the public opinion [13].

The threats of the hybrid war in recent years are felt to a large extent in the Western Balkans, so much so that the security institutions have begun to seriously treat these issues, to extent that they have begun various actions and training of civilian and military personnel in order to prevent them. Such threats are clearly felt in Kosovo, which due to internal circumstances, the regional context and international developments can be very easily exposed to hybrid threats. In most cases, hybrid threats are not easily detected, and even when they are detected, it is often too late to react as the damage they cause is usually irreparable. The developments of computer technology and its impact on society have created the possibility of hybrid warfare without necessarily having to be in an open frontal-classical war since the hybrid war can be developed even in conditions of peace through the financing of propaganda on media, the economic controls, sabotage, interference in cultural and religious matters and interference in elections to influence the determination of the winner of the elections [14].

Conclusion

Coordination among government agencies, non-governmental bodies, and private individuals is key to the execution of hybrid warfare. In hybrid warfare, the essential issue is finding the weak points of the leaders of the targeted states, their armed forces, public order forces, intelligence services, corruption, economic and energetic dependence, etc.

People worldwide have access to so much information, however, Russian attempts to spread disinformation have proven surprisingly effective in Western Balkan too. Freedom of speech is an important human right, but in some cases, Russian-catered media can serve as a method of indoctrinating susceptible individuals who can then carry out more dangerous plans. The use of psychological means of manipulating large swaths of people should not be taken lightly. Hybrid warfare is the future of warfare. Each state (and ideally the entire international community) must embrace this uncertainty in its policy and doctrine. The current lack of legal and political means for addressing cyber operations leaves the international community vulnerable to these kinds of coordinated attacks. Because there are essentially no precedents with which to address cyber warfare, most states shy away from directly addressing a nation's misbehavior in cyberspace.

As it is, there are very few binding legal documents that would serve as guidance when dealing with cyber operations; there is not even any clear legal consensus on whether or not accessing the system of an attacker is permissible. The ensuing debates leave them plenty of time and leeway to continue their aggressive Behavior.

Moscow intends to rule over its neighbors in order to prevent them from getting too close to the Western world, as well as to weaken its key adversaries: the United States, NATO, and the European Union; moreover, it seeks to regain its authority in the Balkans via a victorious hybrid war. In this regard, the faster membership of the Western Balkans in the European Union can become an effective defense against a new round of Russian aggression to expand the war and divert attention from Ukraine. The engagement of civic society is still critical. Unpredictability and ambiguity make it more difficult to recognize hybrid threats. As a result, national leaders and the media have the vital but difficult responsibility of defining these risks so that our societies may stay watchful and robust. Indeed, such explanation is critical for increasing societal resilience and involving civil society, the media, and the IT industry in our efforts to combat hybrid threats. There is a need to foster information plurality, invest in civic awareness via education, and sustain an independent press that reacts quickly to deception. In this regard, EU resources should be made accessible.

Dealing with most types of cyber threats in Kosovo is very difficult and can lead to predictable consequences. Kosovo may be exposed to many other threats due to the economic, social and political situation in the country.

Russian cyber strikes have targeted Kosovo. Kosovo quickly evicted two Russian individuals accused of having ties to Russia's secret services. Such behavior between countries, particularly ones like Russia, is never tolerated nor forgiven. Hybrid threats may present a new chance to further align the Balkans with the Euro-Atlantic community, increase solidarity and transform current political relations. The countries of the Western Balkans should compile a strategy against hybrid threats, strengthen the inter-institutional cooperation within the country and increase the cooperation between the Balkan countries and other partner countries.

References

1. Reid Standish (2018) Inside the European Center to Combat Russia's Hybrid Warfare. Foreign Policy, hybrid warfare: the blending of diplomacy, politics, media, cyberspace, and military force to destabilize and undermine an opponent's government.

2. Deterring hybrid warfare: a chance for NATO and the EU to work together?"

3. Kaplan R (1994) Conference a Roles and Missions of the Special Operations Forces in the Aftermath of the Cold War. Cambridge, USA.

4. Hoffman FG (2007) Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, Arlington, VA, pp: 38.

5. Military Balance (2015) International Institute for Strategic Studies.

6. Barabantseva E, Mhurchú AN, Spike Peterson V (2021) Engaging Geopolitics through the Lens of the Intimate. 26(2): 343-356.

7. Foreign Policy & International Relation (2022) Tirana observatory: Russia's hybrid-war in the-western.

8. Kuczyński G (2019) Russia's Hybrid Warfare in the Western Balkans. Warsaw Institute, Poland.

9. Geopolitica nr. 67 (4/2016), pp: 122.

10. CIA (2018) "Kosovo," The World Factbook.

11. Statistical Office of Kosovo (2009) "Population," Portal of the Government of Kosovo.

12. Kosovo Institute of Statistics annual report, 2021 edition.

13. Prof.asoc.dr at the Public University "Ukshin Hoti" Prizren.

14. Prof at Faculty of Public Safety – Kosovo Academy for Public Safety and UBT College.