HYBRID AND CYBER WARFARE – INTERNATIONAL PROBLEMS AND JOINT SOLUTIONS

Dr Darko Trifunovic[*]

Darko Obradovic[**]

[*] Prof. dr. Darko Trifunović, Director of the Institute for National and International Security, professor at Faculty of Law, Administration and Security, Megatrend University, Belgrade. Dr Trifunovic was elected as guest professor at FUDAN University – Center of American Studies, Shanghai, China. Senior Research Fellow and lecturer at Faculty of Security Studies-University of Belgrade. He is Senior Adviser at the Research Institute for European and American Studies, Greece, Athens. He is a specialist in Security studies, Intelligence & Counterintelligence studies as well as Counter-Terrorism, National and International Security studies. He is a former diplomat (First Secretary of the Foreign Service of Bosnia and Herzegovina at the United Nations). Dr. Trifunovic is the representative for Serbia and Montenegro of International Strategic Studies Association (ISSA); Defense & Foreign Affairs publications; and the Global Information System and he is member of the Advisory Board of the Institute of Transnational Studies, Munich, Germany. The Shanghai Center for International Studies appointed him as the first foreign expert for the Olympic Games (2008) security preparation in China. In 2010, he is engaged in World Expo Security preparation and is a Member. Dr Trifunovic is regular speaker at International Counter Terrorism Institute, Tel Aviv, Israel, and Prof. dr Darko Trifunovic is one of the founding Members of the International Counter Terrorism Academic Community (ICTAC). He has published numbers of academic books papers and articles.

[**] Darko Obradović, born in 1989. Belgrade, graduated Faculty of Security Studies, the University of Belgrade in 2012. Darko is Secretary-General of the Institute for National and International Security. With several years of experience in public service, his main 8-year expertise is in the research of Hybrid Warfare, disinformation counter-measures, national security, and open-source intelligence and counter-terrorism as well. From 2011. until 2018. Darko was worked in an opposition research task force for Political parties during elections in Serbia. Darko is the author of several publications, articles considering geopolitical challenges on Western Balkan and several internal and external reports on disinformation topics.

Abstract: Hybrid warfare is a significant threat to National Security and Countries in last 10 years. Hybrid activities are not new, but environment of cyberspace is completely different than before. We are witnessing a great expansion of the aforementioned fifth combat space, which knows no borders, fences, social or cultural barriers. Hybrid war as a form of endangering the security of sovereign states is primarily based on subversive activities in order to paralyze the state apparatus with the ultimate goal of changing the political leadership. This change of political leadership in the earlier period of history was far simpler and most often began and ended with armed aggression, the use of armed rebellion, or a coup. As modern societies increasingly turn to reliable alliances, mechanisms of collective security, conventional methods have become for quite some time less effective and outdated. The use of disinformation as an integral method of Hybrid Warfare has its roots in the concept of "ideological subversion". Ideological subversion is a term firstly defined by KGB in 1970th. KGB invented "Ideological subversion" as a tool of special warfare against civilians and administrative employees. To make it easier to follow the case study, the

authors of the Hybrid War operation divide it into four phases: Demoralization, Destabilization, Crisis, and Stabilization. For Russia, the Balkans hold significant historic, cultural, and religious connections—shared ties that are actively propagated, and at times exaggerated, by Russian public diplomacy efforts and media narratives.

Key words: Hybrid Warfare, Cyber Warfare, Security, Intelligence, Counterintelligence

Introduction

Hybrid warfare is not class warfare that signifies armed conflict. Hybrid warfare is waged by unconventional means, primarily through the application of information technologies in, so to speak, the newly created space which we define as cybernetic. This area has become very important for the work of security services in terms of defining possible threats coming from such area, but also in terms of conducting special psychological operations according to the marked goals, which might be a state, community, people, vital infrastructure or even important individuals. Hybrid warfare is part of special war, but the term refers to a specific action backed by a foreign intelligence service or services using modern means such as the Internet, social networks, portals and specially designed sites in the cybersphere. In military theories, cyberspace is marked as the fifth combat space next to water, air, land and

space.[1] We are witnessing a great expansion of the aforementioned fifth combat space, which knows no borders, fences, social or cultural barriers. This space directly enters the privacy of each individual and with powerful techniques as well as analytical programs "learns" all the habits of the user. Hybrid actions concentrate on several phases. The first phase is the goal selection phase. The second phase is the phase of preparation of actions. This phase involves gathering all the useful information from history, culture, politics, economics, energy, etc. - in fact, all the information that can greatly affect the interest and awareness of the goal. The third phase is the phase of performing the action.Platforms for transmission of information, misinformation and other contents that are actually launched by the security service are most often used as operational instrument. The fourth phase is the phase of verification of the achieved results and the phase in which, after the achieved goals, one shifts focus from the attack to the defense of the achieved. The era of hybrid operations begins with Russian hybrid activities in Estonia in 2007 and Georgia in 2008. The website of the President of Georgia has been a constant target of Russian hackers. Despite the fact that DDoS attacks passed through US-based IP addresses, experts have detected malware hackers who used to generalize as a "MachBot" DDoS controller. MachBot was written in Russia and is known as a tool of Russian criminal groups[2]. In 2013, the Chief of

---

1. *Laurence Ifrah, "States face new challenges from cyberwarfare and cybercrime", Revue Défense Nationale, Vol. 714, 2008.*
2. *Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," Parameters, Winter*

the Russian General Staff, General Valery Wasiljewitch Gerasimov, presented a new doctrine that was immediately called hybrid warfare[3].

Hybrid warfare as a transnational form of endangering the security of sovereign states

Hybrid war as a form of endangering the security of sovereign states is primarily based on subversive activities in order to paralyze the state apparatus with the ultimate goal of changing the political leadership. This change of political leadership in the earlier period of history was far simpler and most often began and ended with armed aggression, the use of armed rebellion, or a coup. As modern societies increasingly turn to reliable alliances, mechanisms of collective security, conventional methods have become for quite some time less effective and outdated. In this regard, hybrid threats appear as a type of response that is not overly demanding from the point of view of manpower and resources, but also not transparent from the point of view of detecting aggressors.

Hybrid war according to the Cambridge Dictionary: "the use of a range of different methods to attack an enemy, for example, the spreading of false information, or attacking important computer systems, as well as, or

2008,   p.   65, http://strategicstudiesinstitute.army.mil/pubs/para meters/articles/08winter/korns.pdf.
3. *Leslie Hamilton, Philip Webster, The International Business Environment, Oxford University Press, New York, NY, 2016. p.290.*

instead of, traditional military action"[4] According to some authors hybrid threats include a full range of methods of warfare, including conventional capabilities, improper tactics and formations, terrorist acts involving indiscriminate violence and coercion, and criminal offenses[5], including the comprehensive and combined use of special forces, intelligence services, think tanks, NGOs, rebel groups, associations of citizens, the media and intellectuals. What predominantly characterizes hybrid warfare is the use of unconventional forces and means with the use of military principles and tactics. The hybrid war replaced trenches and front lines with social divisions and antagonisms, grenades and bombs were replaced by disinformation, and battalions and infantry were replaced by think tanks, citizens' associations and individuals. What is characteristic of the forces involved in hybrid actions are probably elements deployed and managed by military principles and tactics, forces and means are calculatedly directed to pre-selected targets, diversions are performed and social contradictions are encouraged. Even though the phenomenon is hardly new, what is new and surprising is the "scale of use and exploitation of old tools in new ways[6]."

4. Cambridge Dictionary , https://dictionary.cambridge.org/dictionary/english/hybrid-warfare
5. Frank G. Hoffman, "Hybrid warfare and challenges" , JFQ, 1st quarter 2009, P 36, https://smallwarsjournal.com/documents/jfqhoffman.pdf
6. *JACOBS, Andreas a Guillame LASCONRAJIAS. NATO's Hybrid Flanks, Handling Unconventional*

Some authors often bring hybrid actions into the context of soft and hard power[7], where they present soft power as the basic characteristic of hybrid actions, which in general does not have to be the case. Thus, a party waging a hybrid war does not have to use its values as a necessary container. While the characteristic of soft power is precisely the existence of values as superior to alternatives, soft power is a cultural and social pattern. On the other hand, the use of soft power does not necessarily mean influencing the policy of a sovereign country and decision-makers, while the use of hybrid actions necessarily implies interference in the internal affairs of a sovereign state with the aim of influencing political decisions and top decision-makers.

Since we have defined hybrid warfare, our intention is to focus in this paper on methods of hybrid action by processing a case study - Hybrid warfare in the Western Balkans, the case of Montenegro. By studying hybrid effects in the Western Balkan space, it shows that what dominates them is the abundant use of disinformation and misinformation, which will be the topic of this paper.

Disinformation and misinformation[8] are a key characteristic of the hybrid actions that the

Warfare in the South and the East. NATO Defence College [online]. [cit. 2015-08-01]

7. *Wither, James K. "Making Sense of Hybrid Warfare." Connections 15, no. 2 (2016): 73-87. Accessed December 2, 2020. http://www.jstor.org/stable/26326441.*

8. *Council of the European Union, Complementary efforts to enhance resilience and counter hybrid*

Russian Federation performs against NATO members and areas of geopolitical interest. As part of the placement of disinformation, we have a weaponization of history, culture and traditions, often accompanied by hate speech. In NATO Secretary-General annual report 2019[9], in the section for Hybrid threats is stated: they (Russian Federation) can make political and strategic gains in other ways, such as spreading disinformation, launching cyber attacks, and using deception and sabotage. These hybrid or gray zone activities blur the line between peace and war and are used to destabilize and undermine affected countries. Countering hybrid threats against Allies is a priority for NATO. Allies stand ready to defend each other against hybrid attacks as part of collective defense while recognizing that the primary responsibility for responding to hybrid attacks rests with the targeted nation.

The use of disinformation as an integral method of Hybrid Warfare has its roots in the concept of "ideological subversion". Ideological subversion is a term firstly defined by KGB in 1970th. KGB invented "Ideological subversion" as a tool of special warfare against civilians and administrative employees. "Ideological subversion" is a part of the doctrinal approach and propaganda tool. As a special warfare tool, they intended to use it dominantly against

---

threats - Council Conclusions (10 December 2019)

9. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf

Yugoslavia in the period after 1958. At that time we had the so-called "fifth column" in secret service, military, universities and among journalists. In that period it was defined as ideological propaganda and subversive activities with the goal to overthrow Tito and Yugoslavia regime and integrate it into USSR and Eastern Block. Yuri Bezmenov: "Ideological subversion means always a distractive aggressive activity aimed at destroying the country, nation or geographical area of your enemy".[10]

What experts call disinformation operations today is deeply rooted in the concept of ideological subversion. Russian dissident, count, and defector Vladimir Volkov also deal with the topic of disinformation in his book Disinformation[11] - The media have been transformed from a means of spreading knowledge, enlightenment and information into a means of governing the soul and consciousness of man and people.

Therefore the information, instead of conveying the facts as the truth, regardless weather behind the selection of facts is the choice of the one who conveys them, is transformed into the context in which such facts are placed. Instead of the truth, context is given. Unfortunately, this is not only the case in wartime conditions, but has become a universal practice everywhere in the modern world. Instead of serving the truth, the media are serving the government and power.

---

10. ttps://www.youtube.com/watch?v=wSKr2q9zukQ
11. Vladimir Volkov, "Disinformation", Nas Dom, Beograd, 2013, p 4

To make it easier to follow the case study, the authors of the Hybrid War operation divide it into four phases: Demoralization, Destabilization, Crisis, and Stabilization. The demoralization phase is the initial phase but does not end there. Demoralization activities often represent a continuous activity in all other phases, with the possibility that the demoralization phase can last for years and represent a continuous activity that overlaps with the other three activities. Targets are continuously exposed to the placement of strategic and tactical disinformation. What characterizes the phase of demoralization in terms of the Western Balkan region is that this phase in this area lasts for a hundred years in a row. During that time, the bearers and narratives changed, but the ultimate goals did not change. Influential agency networks have changed narratives and priorities, but never the ultimate purpose. The demoralization phase includes a strong organized activity of placing and multiplying misinformation that seeks to be inserted as an integral part of social discourse and generally accepted truth. Disinformation and misinformation are aimed at weaponizing history, culture, and tradition and deepening the identified social gap, mobilizing public opinion, extorting foreign policy and internal decisions of the sovereign state, creating an environment of open polarization of society[12] and motivation for other forms of action such as unrest, riots, civil disobedience, sabotage and removal of legally elected authorities. In accordance with the methods and tactics of the disinformation operation, they reach their full momentum when

---

12. *Some examples are Moldova, Ukraine, Armenia, North Macedonia, Bosnia and Herzegovina, Montenegro and Serbia*

the media begins to spread misinformation out of their own convictions and ignorance, and when they sincerely believe in them. Through cyberspace, it has never been easier to place disinformation and misinformation from the point of view of selecting the target population, performance control, and analytical cross-section of achieved goals. In this phase, pre-prepared materials are placed, the complexity and difficulty of the defense in this phase represents the potential of social networks with all their specifics. The destabilization phase continues to rely on the demoralization phase, with a conceptual change involving stably formed and active pressure groups and agents of interest. Pressure groups embodied in think tanks, citizens' associations, political parties and individuals are resolutely engaged in shaping political goals and polarizing society through formalizing action, organizing demonstrations, civil disobedience, abuse of power, creating scandals, openly demanding political demands and causing riots and unrest. Depending on the state's response, this phase can last from a few days to several months. Instead of a large-scale military invasion, the attacker[13] aims to target and undermine the subject by other methods, often involving the use of disinformation campaigns, subversive intelligence, cyber-attacks, sabotage, or (not only) political support of separatist or other groups advantageous for the attacker. Whether this phase can gain additional dynamics embodied in the next phase of the Crisis depends on the readiness of the state and its

---

13. *Richterová, Jitka, NATO & Hybrid Threats, Asociace pro mezinárodní otázky, Prague, 2015, p. 5.*

response, and especially on strategic communication.

The Crisis phase takes place successfully when the listed subjects gain the potential to paralyze society, to impose their activities in public discourse and maintain the ability to maintain continuous riots, demonstrations, riots, fierce conflicts with law enforcement agencies, formal or informal occupation of institutions and change of government and foreign policy, as well as country orientation. In this phase, it is characteristic that other forces for hybrid actions are included in the Hybrid operations, such as special units and rebel groups, for example Crimea, Eastern Ukraine, Transnistria. This phase can last continuously for years. Crimea began as a covert military operation, combining ambiguity, disinformation, and the element of surprise at the operational level with more traditional aids such as electronic warfare. The annexation was completed by a traditional military invasion and occupation of the peninsula, using Russia's airborne, naval infantry and motor rifle brigades. This operation was unique, because Russia's Sevastopol naval base, status of forces arrangements in Crimea, and additional agreements on transit of troops in Ukraine enabled deployments and tactics that would not otherwise have been possible.[14]

The Stabilization phase represents the crown of success of all previous phases, after which the bearers of hybrid actions achieve their geopolitical goals, which become a reality on

---

14. Michael Kofman and Matthew Rojansky, *A Closer look at Russia's "Hybrid War", No. 7 I April 2015, Wilson Center*

the ground. For that, we have the most recent examples of the occupation of Crimea and Eastern Ukraine, and the upcoming crisis in Moldova.

Hybrid warfare as an international problem on the Western Balkans

For Russia, the Balkans hold significant historic, cultural, and religious connections—shared ties that are actively propagated, and at times exaggerated, by Russian public diplomacy efforts and media narratives.

The hybrid effects on Western Balkans as stated have their continuity for more than a hundred years. The main goals are to prevent the full integration of the Western Balkans into the EU and NATO with the abundant creation of social conflicts with the aim of creating a set of dysfunctional states and governments, as guarantees for permanent isolation integrated into a hybrid form of "alliance" through Eurasian Union and OACS membership.

The set of activities, measures and actions were skillfully prepared and organized by the intelligence services of the Russian Federation. Through proxies embodied in think tanks, citizens' associations and individuals, the dominant zone of influence are cyberspace-social networks, media and portals that create and exploit social contradictions, with the aim of antagonizing Western Balkan space towards EU-Atlantic integration.

Hybrid effects on Western Balkan represent a multidimensional activity whose carriers include:

1. State actors
2. Non-state actors

According to the areas of activity, it is indicative that all areas of social life are networked. According to this classification, we can divide them into the following zones of interest through social groups:

- Hooligan and team support groups

- Low census political parties

- Minor political movements

- Cultural movements/ Churches

- Individuals such as intellectuals, journalist and artists

- News portals and other media

Education is an area of activity that has become very pronounced in the last two years. Through the scholarship system, students are sent to study at Russian universities intended for civil servants.

By reviewing the events from the previous period, we can see that the activities of the listed pressure groups supported by state actors are able to prevent and paralyze political and foreign policy decisions. Examples are numerous about the potential for creating a huge social conflict over NATO and EU membership, to foreign policy pressures - Facebook Maria Zaharova "If you are invited in the White House and the chair is set as for interrogation, sit as presented in the photo no.2, whoever you are. Trust me".[15]

---

15. *https://www.bbc.com/serbian/lat/srbija-54055450*

What is encouraging in present situation are the decisive moves that the leadership of the Western Balkan states take despite strong threats to their political survival. First of all, the membership of Montenegro and N. Macedonia in NATO and the Washington Agreement for Serbia. The Washington agreement in the case of Serbia immediately provoked a reaction from the Kremlin, but also attempts at a coup in Montenegro as well as threats of demonstrations and riots in Skopje.

That hybrid actions on the Western Balkans represent the potential for transnational endangerment can be seen through the case of the Russian factory of bots and trolls that operated from N. Macedonia throughout Europe. Mark Zuckerberg once stated - " Bots from Macedonia tried to influence the outcome of the elections in the American state of Alabama by using fake profiles and placing fake news. We neutralized those attempts. All this is not quantum physics, but it is just a lot, a lot of work for us that we have to do. "[16]

Russian Federation's hybrid actions on Western Balkans carry their foreign policy implications which we could see in the example of Montenegro. Montenegro faced an attempted coup and an assassination attempt on President Djukanovic to prevent NATO membership.[17]

---

16. https://www.b92.net/info/vesti/index.php?yyyy=2018&mm=03&dd=22&nav_category=78&nav_id=1372325
17. https://www.bbc.com/news/world-europe-48212435

In all these cases, we see that through disinformation and misinformation, public opinion is strongly polarized and thus prevents the political integration of the Western Balkan into the EU and NATO. An example of this is a recent public opinion poll according to which citizens perceive the Russian Federation as the largest donor in relation to the EU.

Hybrid Warfare on Western Balkan methods and techniques are weaponization of historical interpretation, tradition, emotions, international relation, religion, nationalism, active measures, disinformation and fake news. Public advocacy subjects and individuals as channels for the weaponization of history are: Individuals – mostly intellectuals Internet and Social Networks Conventional channels- events, books, newspapers Exploitation of history are based on usage of fake history interpretation, usage of true fact in certain moments and contexts. The purpose is to deeply and continuously antagonize and present Russia as the savior of orthodox Christianity and the "New Rome". These activities are mostly in connection with hate speech. The weaponization of religion we sow on Montenegro example (more in the case study). War in Former Yugoslavia and Kosovo is the strong lever which Kremlin use to place narrative against western values and euro-Atlantic integration. Disinformation and fake news are the dominant activity mostly present on the internet and social network, in the last few years traditional channels as events are increasing (on Universities and para-political NGOs), but mainstream newspapers are also significantly involved.

Brief case study Montenegro vs Religion Freedom

In the events of 2019 and 2020 in Montenegro, we can clearly see the pattern of application of hybrid operations through the phases of demoralization, destabilization, crisis and stabilization. In phase of demoralization was held a series of events on Universities mostly about „Position of Serbs and Serbian Orthodox Church in Montenegro"[18]. Presented narrative was imaginary endangerment of Serbian Orthodox Church, identity topic and dilemmas from 19th century. Russian Federation misused Serbia as hub for those operations simultaneously with activities in Montenegro. Russian strategists estimated that religious mater can be very well exploited and it will mobilize large public support and individuals. So they have started with preparation activities almost one year before election period in Montenegro. The activities started with the organization of a series of tribunes on the Serbian identity and position of the Serbian Orthodox Church in Montenegro by organizations connected to the official channels with the Embassy of the Russian Federation.

---

18. *https://www.instagram.com/p/By8WlV8oyLb/*
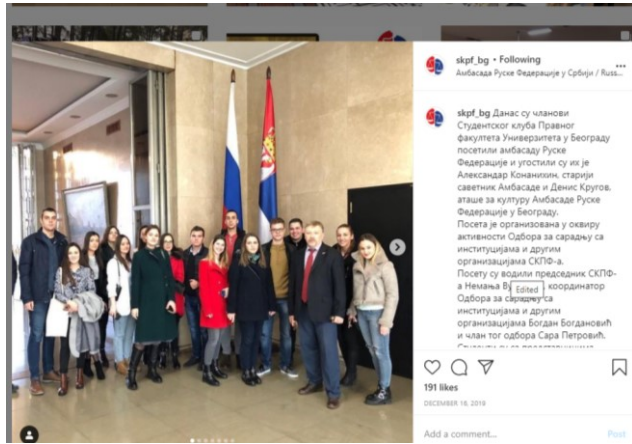
Student Organization – Student's Club of Faculty of Law in one of numerous visits to Russian Federation in Belgrade, with diplomat Aleksandar Konanihin on picture

On picture is archbishop of Serbian Ortodox Joanikije Church with the leader of one Student Organization – Student's Club of Faculty of Law on

one on several events organized with topic about endangerment of Serbian Church and identity in Montenego

The demoralization phase included a huge presence of false news, hate speech, misinformation and calls for defense against an imaginary enemy, all in connection with NATO membership in Montenegro as a form of threat by itself. In the campaign of spreading false news and disinformation, the portal www.in4s.net played a strong leading role in the cycle of creating misinformation.

The portal presents itself as a journalist, without an official registration in the media register, without an imprint deprived of any responsibility. The same portal was the creator of a lot of content designed to provoke an emotional reaction from readers, using the abuse of historical contexts and linking the President of Montenegro to the fascist regimes of World War II[19]. Side by side with the pro-Kremlin Sputnik, IN4S actively placed disinformation. The cases of misinformation by these two portals were largely documented by the Digital Forensic Center from Podgorica[20].

From a phenomenological point of view, misinformation has been shown to be crucial in the demoralization phase in order to deepen social gaps, polarize society as a whole but also to mobilize actors in Montenegro and abroad in order to maintain false perceptions

---

19. *https://www.in4s.net/jovanovic-milo-po-ugledu-na-ndh-zeli-da-rusi-i-otima-srpske-svetinje-u-crnoj-gori-video/*
20. *https://dfcme.me/*

and narratives in order to create an atmosphere of survival and false narratives.

The destabilization phase began with the organization of demonstrations called "Itije". At this point we have the classic abuse of religious rites and religion as a whole by church dignitaries. From a psychological and emotional point of view, the organizers called the demonstrations against the Law on Freedom of Religion liturgies based on religious rites that have nothing to do with civil disobedience and political demands. The slogan of the demonstration was

"We do not give the Holy."

During the destabilization phase, we gained new quality in terms of demands that were extended to political demands for overthrowing of the legitimate authorities of Montenegro. The placement of content ranged from hate speech to disinformation and misinformation. The main narratives were aimed at linking NATO membership to membership in a fascist coalition from World War II, anti-Serbian intentions, denial of democracy and civil society. As the election process progressed, the organizers slowly entered the phase of the Crisis, during which there were sporadic clashes with the police - quote, but also with the increasing intensity of spreading false news.

Pro-Russian para-political organization and media statements against Montenegro and Euro-Atlantic community:

EXAMPLE 1:

Milo is building a NATO church on the foundations of the Serbian Orthodox Church.

Instead of baptismal glory, he will celebrate Javier Solana, instead of incense, he will use depleted uranium. Yesterday Dachau, today Montenegro. It is a concentration camp for Serbs in which they beat bishops, arrest MPs and persecute the people, "said Milica Đurđević from ultra-right pro Russian party-Zavetnici.[21]

EXAMPLE 2:

MILO ATTACKED THE Serbian Orthodox Church (SOC) BECAUSE OF AMERICA - Hodges then said that the countries of our region "should be provided with support and protection from Russian pressure", and that "Serbia should be helped to resist the pressure of the SOC, which is tied to Russia".[22]

EXAMPLE 3[23]:

---

21. https://www.alo.rs/vesti/politika/podrska-za-srbe-i-svetinje-u-crnoj-gori/276675/vest
22. https://www.intermagazin.rs/milo-je-zbog-amerike-udario-na-spc-a-ovo-je-razlog/
23. www.dfcme.me

On left side we can see twit from opposition leader in Montenegro Marko Milacic, where is made statement that police crushed a baby, and on right side we see that picture is from medical advertisement.

From the presented examples we can see that as the phases of demoralization, destabilization and crisis are moving away, so the intensity of false news, disinformation and misinformation is increasing. The bearers of hybrid warfare act together as amplifiers along the lines of social life - culture, history, tradition, economy and security. With a clear characteristic of stimulating negative emotions and deepening antagonisms in order to divide society.

In the crisis phase, the hybrid war in the case study of Montenegro has the following characteristics:

1. Massive rallies ,

45

2. Posibility to impact mainstream media with fake news and disinformation,
3. Social unrest,
4. Radicalization of larger population groups,
5. Possibility to disseminate propaganda, fake news and disinformation by controlled media and news portals,
6. Mobilization of voters and psychological impact on their decisions,

The stabilization phase is still ongoing in the case of Montenegro, its characteristics are the successful completion of the hybrid operation with the following outcomes:

1. Change of pro-western government
2. Foreign policy turn of Montenegro's policy
3. Strengthening Russian influence in Montenegro
4. Re awaken old Joseph Stalin plan for creation of Balkan Union under Russian control.

As the events and outcomes in Montenegro are still current, it remains for us to monitor the outcomes

Conclusion

Hybrid threats are definitely transnational security challenges, which abuse territories of several countries. Potential of hybrid attacks is very large. Countries should establish counter-hybrid teams and form international alliances as response to aggressive Russian activities within Europe. The case of Montenegro, as an example, should alert Western Balkans' countries. It also lectures countries in general on the need to impose multi-sectorial approach in response to such threats.

Covid19 consequences will further boost a potential for disinformation and hybrid activities as tools for destabilization of Western Balkans and EU as well. Early response mechanism should include international cooperation in suppressing organizations and individuals which are proven hybrid actors. EU and NATO mechanism of cooperation should include mapping of such organizations and individuals, with the result of sanctioning them and forbidding entrance to EU and NATO countries. That would be a required mechanism to prevent such organizations and individuals to operate, travel, establish connections and promote harmful content and activities. Social network operators should extend and improve mechanisms for preventing deliberate misuse of freedom of speech. Based on presented points we can conclude that serious efforts are needed to design proper response to Hybrid and Cyber Warfare with respect for human rights and freedom of speech.

LITERATURE

1. *Cambridge Dictionary*
2. *Council of the European Union, Complementary efforts to enhance resilience and counter hybrid threats- Council Conclusions (10 December 2019)*
3. *Frank G. Hoffman, "Hybrid warfare and challenges" , JFQ, 1st quarter 2009*
4. *JACOBS, Andreas a Guillame LASCONRAJIAS. NATO's Hybrid Flanks, Handling Unconventional Warfare in the South and the East. NATO Defence College*
5. *Laurence Ifrah, "States face new challenges from cyberwarfare and cybercrime", Revue Défense Nationale, Vol. 714, 2008.*

6. *Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," Parameters, Winter 2008*

7. *Leslie Hamilton, Philip Webster, The International Business Environment, Oxford University Press, New York, NY, 2016*

8. *Michael Kofman and Matthew Rojansky, A Closer look at Russia's "Hybrid War", No. 7 I April 2015, Wilson Center*

9. *Richterová, Jitka,NATO & Hybrid Threats, Asociace pro mezinárodní otázky, Prague, 2015*

10. *Security Science Journal, http://www.securityscience.edu.rs/*

11. *Vladimir Volkov, "Disinformation", Nas Dom, Beograd, 2013*

12. *Wither, James K. "Making Sense of Hybrid Warfare." Connections 15, no. 2 (2016)*

13. *https://www.nato.int*

14. *www.bbc.com*

15. *www.b92.net*