Hybrid Threats and Counter-Hybrid Solutions: A Comparative Case Study Analysis of Croatia, North Macedonia, and Bosnia and Herzegovina

ROBERT MIKAC, MARINA MITREVSKA AND MIRZA SMAJIĆ

sciendo

Politics in Central Europe (ISSN 1801-3422)
Vol. 18, No. 3
DOI: 10.2478/pce-2022-0017

Abstract: *Hybrid threats are not new security challenges, but they are becoming more and more pronounced, primarily due to the situation in Ukraine, where multiple hybrid activities are underway by Russia. As central actors in the European security architecture, the European Union and NATO recognise that both organisations, their member states and other countries in Europe are exposed to various forms of hybrid threats. However, this ability to recognise hybrid threats and especially the development of counter-hybrid solutions is an open question for some smaller countries. In order to investigate the above, this paper focuses on hybrid threats and counter-hybrid solutions by analysing the state of affairs in Croatia, North Macedonia, and Bosnia and Herzegovina. Our goal is to explore this area and answer the following research questions: What hybrid threats are Croatia, North Macedonia, Bosnia and Herzegovina exposed to? How do they deal with them? What counter-hybrid solutions are being developed?*

Key words: ***Hybrid threats, counter-hybrid solutions, Croatia, North Macedonia, Bosnia and Herzegovina***

Introduction

Modern states are exposed to numerous security risks and challenges every day. One of the phenomena they encounter also applies to hybrid threats. According to the European Commission (2022a):

A hybrid threat refers to when, state or non-state, actors seek to exploit the vulnerabilities of the EU to their own advantage by using in a coordinated way

a mixture of measures (i.e. diplomatic, military, economic, technological), while remaining below the threshold of formal warfare. Examples are the hindering of democratic decision-making processes by massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors.

The North Atlantic Treaty Organisation has a similar definition:

Hybrid threats combine military and non-military, as well as covert and overt means, including disinformation, cyberattacks, economic pressure, and deployment of irregular armed groups and use of regular forces. Hybrid activities are often used by adversaries because they realise they cannot prevail in a conventional conflict with NATO, or broadly with the West, or even compete politically, militarily or economically (Cattler 2021).

On the same track is the European Centre of Excellence for Countering Hybrid Threats (2022):

The term 'hybrid threat' refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision--making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.

At the beginning of the research, we must point out that by studying hybrid--base literature, we did not find a unique definition of hybrid threats, but rather collective characteristics of different measures that together pose a severe threat to specific entities (usually states that are threatened, but it can also be different organisations' and institutions' critical infrastructure facilities, etc.).

It is important to distinguish different 'hybrid' terms:

Hybrid threat is a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat. Hybrid conflict and hybrid war are two specific categories whereby some hybrid tactics are used by a state to achieve its strategic ends. Hybrid conflict is a situation in which parties refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of an attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives. Hybrid war is a situation in which a country resorts to overt use of armed forces against another country or a non-state actor, in addition to a mix of other means (i.e. economic, political, and diplomatic) (Think Tank of the European Parliament, 2015).

While most countries are exposed to certain types of hybrid threats, some – like Ukraine at the time of writing – are at risk of open hybrid warfare.

The following should be taken into account when considering hybrid threats:

Hybrid always describes a combination of two or more tools or actions. Hence, we should not use the term when we are just describing a series of cyberattacks or a single disinformation effort. Only when several tools are applied together is the word 'hybrid' really appropriate (Rühleu 2021).

As the most obvious examples of hybrid threats, we can cite a few examples:

Terrorism: Terrorist organisations like Boko Haram, Al-Qaeda in the Arabian Peninsula (AQAP) and ISIL/Da'esh operate across the territories of many countries, and employ a variety of economic, military and technological tools to achieve their political goals.

Cybersecurity: The operations of state-affiliated hackers from Russia and China and the use of cyber-weapons are facilitated by difficulties with the attribution and the absence of norms of state behaviour in cyberspace.

Organised crime: Armed criminal groups and drug cartels in Mexico resort to violence in the fight over territory and economic profits. Erosion of security, in turn, has a negative impact on the Mexican economy.

Maritime disputes: China is pursuing its aims in the South China Sea by combining economic and military pressure with extensive land reclamation projects in the Spratly archipelago.

Space: Constraints on use of orbital space (and access to satellites) resulting from space debris – created, among other things, by anti-satellite missile tests.

Resource scarcity: Resource-dependency between countries is increasingly used for political purposes. In 2010, China blocked exports of raw materials to Japan in response to the arrest of a Chinese fishing boat. In 2011, India's refusal to adopt a water-sharing agreement with Bangladesh put additional pressure on bilateral relations.

Covert operations: Russia's strategic use of special forces (i.e. 'green men') and information in Ukraine. (Think Tank of the European Parliament, 2015)

As can be seen, hybrid threats are realised in many areas and different parts of the world. Due to their geostrategic and geopolitical position, some regions are more exposed to hybrid threats; one such region being Southeast Europe and, more specifically, the Western Balkans, where countries are struggling with numerous internal challenges (such as severe corruption, weak and inefficient state institutions, unfinished transition processes, slow development, demographic aging, permanent emigration of young population, etc.) and external pressures coming from global and regional powers that project their interests in the area. In such circumstances, hybrid threats pose a significant additional security challenge for all states. Moreover, this area is subject to various influences due to its specifics. 'Few regions in the world can claim a cultural, religious and demographic diversity richer than the Western Balkans' (NATO Parliamentary Assembly 2018: 1).

Hybrid threats are visible in Southeast Europe and, more specifically, in the Western Balkans: the debt trap diplomacy of China, Turkish authoritarian propaganda, violent extremism supported by the Gulf countries and Iran, disinformation warfare conducted by Russia, as well as the rising far right violent extremism identified in Serbia, Bosnia and Herzegovina, and Croatia (Rrustemi et al. 2019: 3). According to the NATO Strategic Communications Centre of Excellence (2020: 34–35), Montenegro is vulnerable to hybrid threats and hostile information campaigns; in North Macedonia there is a visible presence of hybrid threats coupled with underdeveloped societal resilience; Kosovo is assessed as not being resilient enough to face hybrid threats; Serbia also lacks resilience to hybrid threats; Bosnia and Herzegovina has ineffective state actions against hybrid threats. Miroslav Mitrović (2018: 39) states that Balkan states are exposed to non-military but hybrid influence of outside powers. Kosovo has zero resistance against possible future hybrid attacks; Albania, and Bosnia and Hercegovina are vulnerable regarding hybrid threats; Montenegro and Romania are potentially under hybrid influence campaigns; Bulgaria, Croatia, North Macedonia and Serbia are exposed to similar hybrid acts. Lack of resilience differs from country to country, but overall author conclusions indicate that all four abovementioned countries are potentially exposed to hybrid actions. Moreover, Slovenia has the most developed resilience capabilities.

Based on various sources, the main hybrid actor in Southeast Europe and, specifically in the Western Balkans, is Russia, but it is not the only one. Hybrid influence, or hybrid threats, come from Russia, Turkey and Saudi Arabia in the EU enlargement process of the Western Balkan countries (Falon et al. 2018: 9). 'The Western Balkans constitute quite a welcoming ground for Russian soft power efforts and propaganda, the aim of which is both to enhance Russia's image as an influential player and when possible to undermine its rivals' leverage' (Ibid: 38). Leaked intelligence documents have suggested that Russian state-sponsored agencies in the Western Balkan region have worked with Russian intelligence in an effort to sow discord in North Macedonia and put a brake on this country's rapprochement with the West (Harding et al. 2017). Russia is involved in carrying out hybrid warfare against pro-Western authorities in Montenegro, North Macedonia and Kosovo while its support for Bosnia's Serb separatists poses a threat to state structures. The Kremlin's undertakings are aimed at drawing Serbia away from Western institutions (Warsaw Institute 2019: 3). Probably the strongest example of Russia's hybrid activities in the region is its involvement in the 2016 coup attempt in Montenegro and preventing it from joining NATO (Guardian 2016; Hopkins 2017; BalkanInsight 2018; Warsaw Institute 2019: 13; Greene et al. 2020: 14–15).

According to the review so far, we can conclude that all the countries in the observed region are exposed to various forms of hybrid threats. Due to academic precision, it should be noted that hybrid threats do not come only from the ac-

tors mentioned so far, but have also been recorded from 'friendly' countries, as well as countries in the region. To give a focus to the research, the paper will provide a comparison between Croatia, North Macedonia, and Bosnia and Herzegovina (three countries in the same region, where Croatia is a member of the EU and NATO, North Macedonia is a member of NATO, while Bosnia and Herzegovina has not yet achieved membership in any of these organisations), with the following research question: What hybrid threats are Croatia, North Macedonia, and Bosnia and Herzegovina exposed to? How do they deal with them? What counter-hybrid solutions are being developed?

In order to structure the research, the *Introduction* is followed by a second part titled *Methods*, in which the research design of this paper will be presented. The next part is *Case Study: Croatia*, which will analyse the state of hybrid threats and counter-measures in Croatia. What follows is *Case Study: North Macedonia*, which, as in the previous case, will analyse the state of hybrid threats and counter-measures in North Macedonia. Finally, the same approach will be used for the part on *Case Study: Bosnia and Herzegovina*. *Discussion* is the following chapter where key research results will be presented and compared. After the analysis, the aggregate indicators and comparison will be presented in the *Conclusion*.

Methods

The research design of this paper consists of a comparative qualitative analysis of a case study of Croatia, North Macedonia, and Bosnia and Herzegovina. 'Comparative design is one of the most important research designs in political science, but the main difficulty with comparative design is finding comparable cases' (Burnham et al. 2006: 58–59). To respond to the stated challenge of designing comparative research, researchers opt for two basic designs: first, the most similar cases design; second, the most different case design (Ibid: 65). Qualitative research methods are a generic term that refers to a whole range of techniques, such as observations, participatory observations, interviews with individuals and/or focus groups, and other techniques. These methods seek to explain the context, meaning and different processes (Devine 2005). Regarding case study, Yin (2007) states that the case study is an empirical study referring to a contemporary phenomenon within its real-life context. An approach will be used as a comparative analysis of the most similar cases design because Croatia, North Macedonia, and Bosnia and Herzegovina have multiple features in common, i.e. all three countries have very similar political paths and histories – they were all socialist republics within the former Yugoslavia. With the disintegration of Yugoslavia, all three socialist republics followed a difficult path of independence, state and institution-building, as well as joining the Euro-Atlantic integration. Geographically, they belong to the same region, while the size of

the territory and the number of inhabitants are pretty similar. These are small countries with limited levels of capabilities but also opportunities. Therefore, their comparison through most similar design cases is justified. The qualitative analysis will include official documents, academic and media sources for each country. In addition, in-depth interviews with security experts from each country analysed will be included in the analysis.

Case Study: Croatia

An analysis of the hybrid threats Croatia is exposed to will be presented through a three-level analysis. The first level is Official Acknowledgement of Hybrid Threats; the second level is Potential Hybrid Threats; and the third level is Activities that may be Related to Hybrid Threats. The analysis ends with a cross-section of Planned and Undertaken Counter-Measures of the state.

Official Acknowledgement of Hybrid Threats

Official Acknowledgement of Hybrid Threats represent threats that the state's official institutions have qualified as such. We use official documents to analyse those. *The National Security Strategy of the Republic of Croatia* recognises hybrid threats as a part of activities that take place in the wider area to which Croatia belongs, but also the Strategy in two places states that Croatia is as well directly threatened by hybrid threats. In the first case, 'in some countries a defamatory campaign directed against Croatia has been underway for years, with all the characteristics of hybrid and special action, meaning planned, permanent and systematic activities supported by state bodies' (Croatian Parliament 2017: 13). In the second case, 'Croatia is exposed to various forms of hybrid operations that include elements of non-conventional, asymmetric, and cyber actions, both independently and as a part of the Euro-Atlantic integrations. The objective of such operations is to exploit Croatia's vulnerability, weaken its sovereignty and independence, undermine democratic values and freedoms, destabilize state institutions and damage the reputation and influence of Croatia' (Ibid: 14). The next significant source of insight into hybrid threat exposure is Croatian Security and Intelligence Agency Public Reports. Starting from the last published Public Report to the earlier ones, we will highlight the key parts related to hybrid threats. In Public Report 2020/21 hybrid threats are mentioned in the economic sphere and exposure of Croatia to 'the risks associated with intelligence and hybrid operations directed against Croatian or common European interests under the guise of legitimate economic activities' (Security and Intelligence Agency 2021: 22). In the second case, where Russia is directly mentioned as a hybrid actor that threatens the West (which means that this also applies to Croatia), it is stated that: 'The relations with the West have been strained because of indi-

cations of Russian engagement in physical elimination of political opponents, hybrid operations directed at Western states, and cyberattacks originating on Russian territory' (Ibid: 27). In Public Report 2017, Croatia's exposure to hybrid threats is stated in the context of foreign intelligence activities which are 'directed at decision-making in the Republic of Croatia. These activities bear elements of hybrid warfare, including broadcasting "fake news" into the public arena and attempts to undermine the international reputation of Croatia' (Security and Intelligence Agency, 2017: 12). Other Security and Intelligence Agency Public Reports mention hybrid threats and other forms of hybrid activities in a broader context, not mentioning Croatia's direct exposure, but certainly linking it through the threats faced by the organisations (EU and NATO) to which it belongs.

Potential Hybrid Threats

Potential Hybrid Threats represent assumptions about possible hybrid threats that have been developed within the academic community and have not been confirmed by official institutions. Nikola Brzica (2019: 27–28) believes that during the War of Independence ('Homeland War') from 1991 to 1995, Croatia was exposed to hybrid threats and hybrid war by Serbia and its proxy forces in Croatia, and Bosnia and Herzegovina. Željko Crvtila (2017: 14–17) agrees that Croatia was exposed to hybrid threats and a hybrid war by Serbia during the War of Independence. The same author cites recent examples of the use of hybrid threats against Croatia, such as an attempt to portray the country as a pro-fascist state, prevention of the appointment of a Defense Minister by insinuating the war crimes he commanded during the War of Independence, all the way to the takeover (purchase) of public media and media in Croatia by companies and individuals who come from (un)friendly countries and who then undermine Croatia in the media space (Ibid: 14–17). Gordan Akrap (2019: 39) connects hybrid threats to Croatia, among other things, with the threats to national critical infrastructures.

Hybrid Threats

Activities that may be Related to Hybrid Threats refer to a set of different processes and measures that have indications to be characterised by hybrid threats, but they need to be researched and reviewed, and above all, it should be proven that they belong to hybrid threats. We should be especially careful not to call things by the wrong name. Therefore, everything that is stated in this section represents hypothetical assumptions that serve for open discussion. We will give two examples, the first of which refers to the activities carried out by the official policy of Hungary towards Croatia. The Hungarian state oil company

MOL, by purchasing a controlling stake in INA (the state oil company of Croatia), has started managing INA in a way that some experts believe is targeted to reduce its value, does not invest enough in the development of capacity and capabilities, and tries to stop the work of individual plants. In this way, from a once respectable regional company that was present in several countries, INA became a subsidiary which is completely dependent on the decisions made in Budapest. In connection with the above, it is necessary to point out the lawsuit before the Croatian courts in which the former Croatian prime minister was convicted of 'selling INA' to the Hungarians by a criminal act of corruption in cooperation with the president of the board of MOL. The president of the board of MOL is inaccessible to the Croatian judiciary for questioning, while Hungary refuses to extradite him, as well as refusing to actively participate in supporting the trial process. Furthermore, top Hungarian politicians (such as the prime minister himself) occasionally present theses in the media as well as 'historical maps' in which they allude to having pretensions and appropriate parts of Croatian territory.

Another example refers to the activities of certain groups or individuals from Italy who also show 'interest' towards the parts of the territory of Croatia. Similar to the Hungarians, they sought a stronghold in historical circumstances and the fact that during certain periods of Italian imperialism, parts of Croatia were under Roman rule. It is especially important to highlight the position of the president of the European Parliament, Antonio Tajani (Italian politician, journalist and former Italian Army officer, who served as president of the European Parliament from 2017 to 2019), from February 2019 when he finished his speech on the National Memorial Day of the Exiles and Foibe commemoration in Basovizza (Trieste) with the conclusion that the Croatian regions of Istria and Dalmatia belong to Italy (Veljković 2019). Just like Croatia, Slovenia is exposed to the challenges from historical maps published in Hungary and Italy from time to time by various institutions, groups and individuals showing parts of the country as the territory of Hungary and Italy. The prime minister of Slovenia, Marjan Šarec, reacted to this with the following words: 'A blind person is one who does not see that Nazism and Fascism are being reborn in our neighborhood' (Šoštarić 2019).

Planned and Undertaken Counter-Measures

Planned and Undertaken Counter-Measures refer to the development of the ability to counter all forms of hybrid threats to which Croatia, its institutions, critical infrastructure, society and citizens are exposed. On that trail, 'national capabilities will be developed to counter and defend against hybrid operations carried out either by states, organisations or individuals across a wide spectrum (diplomatic, political, information, military, economic, financial, intelligence

and legal)' (Croatian Parliament 2017: 27). As an example, we can highlight the establishment of the Security and Intelligence Agency Center for Cyber Security, with the aim of protecting the national cyberspace throughout 2019. It can be assumed that hybrid threats coming through cyberspace will be monitored and analysed in the mentioned centre. It is especially important to point out that due to its own limited capabilities in all areas, Croatia pays significant attention to cooperation, 'enhanced through existing frameworks intended for building resilience against hybrid threats in NATO and the European Union' (Ibid: 27). In 2019, Croatia became the 19th member of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), which admits only EU and NATO member states. In 2020, Croatia participated in the international NATO exercise 'Cyber Coalition 2020', which included defence against malware and hybrid challenges, and in 2021 in the EU exercise 'Integrated Resolve', which aimed to train reactions in case of hybrid warfare.

Case Study: North Macedonia

An analysis of the hybrid threats North Macedonia is exposed to will also be presented through three levels. The first level is Official Acknowledgement of Hybrid Threats; the second level is Potential Hybrid Threats; and the third level is Activities that may be Related to Hybrid Threats. The analysis ends with a cross-section of Planned and Undertaken Counter-Measures of the state.

Official Acknowledgement of Hybrid Threats

Official Acknowledgement of Hybrid Threats refers to threats that the official institutions of the state have qualified as such. Upon their review, we will use official documents adopted by state institutions. Namely, according to the 2020 *Defence Strategy of the Republic of North Macedonia,* 'the most significant risks we [North Macedonia] face are from asymmetric, hybrid and cyber threats and other non-military threats, including those posed by non-state actors, natural disasters, technological disasters, epidemics and climate change' (Ministry of Defence 2020: 6). With respect to the identified security challenges, threats and risks, the defence system of the Republic of North Macedonia will build capacities and capabilities to respond accordingly (Ibid). Another important source of insight into the exposure of hybrid threats is the *2021 Strategy for Building Resilience and Tackling Hybrid Threats,* which states that 'hybrid threats refer to a combination of malicious and subversive activities, conventional and unconventional methods (diplomatic, military, economic, technological) which are utilized in a coordinated manner by state and non-state entities in achieving specified goals' (Government of the Republic of North Macedonia 2021: 5).

Potential Hybrid Threats

Potential Hybrid Threats have been detected on several occasions in North Macedonia, and they have been used as an 'umbrella', covering a wide range of emerging forms of security threats that may come from either state or non--state actors, and for which there is difficulty in proving their attribution and accountability. The first example is the fact that a great deal of misinformation and fake news is circulating in the information space in North Macedonia. This is being confirmed by the cyberattacks during the election cycle for the 2020 parliamentary elections, when the target of the attack was the State Election Commission and its website, which did not work for three days, and therefore, the public did not have access to the voting results. Hristijan Ilievski (2022: 1) believes that in the past 2–3 years, North Macedonia has been the target of cyberattacks aimed at penetrating the institutions, which has contributed to an erosion of citizens' trust in them. He argues that other such examples were the attempts for hacking the National Bank website, as well as the websites of the Ministry of Education and Science, and the Ministry of Health. The same author also cites a specific example of potential hybrid threats towards North Macedonia, such as the veto from neighbouring Bulgaria and the issue of European integration of North Macedonia. Ilievski further states that support for the European Union membership in recent years has declined from 92 % in 2011 to just under 70 % in 2022. Keeping in mind these numbers, the forces that oppose the accession of North Macedonia into the European Union will undoubtedly use the dissatisfaction of the population and the 'enlargement fatigue' of the European Union to their advantage, in order to achieve influence within political frameworks. Additionally, we can take an actual example of this from neighbouring Bulgaria, where Prime Minister Petkov started the topic of the Russian Federation interfering in the destabilisation of Skopje-Sofia relations through their spies and intelligence officers who worked in the Bulgarian Security Agency and aimed to block EU enlargement in this area. Marjan Nikolovski (2020) believes that hybrid threats would directly endanger security, and one of the ways is communication with top politicians. An example is the non-existent telephone conversation between prime minister Zoran Zaev and a third party. Marjan Zabrčanec, the advisor to prime minister Zoran Zaev, announced that a hybrid attack on the prime minister's office was discovered, in which the identity of the young eco-activist Greta Thunberg was abused. Russian pranksters Vovan and Lexus had published a fictional conversation between prime minister Zoran Zaev and activist Greta Thunberg.

Activities that may be Related to Hybrid Threats

In North Macedonia, there are a set of different processes and measures that have indications to be characterised as hybrid threats. We will list a few which are present in the country and have been demonstrated so far through several sectors, and could be systematised as threats coming through diplomacy, economy, the information and telecommunication sector, and the security sector. In terms of diplomacy, the Macedonian authorities have so far officially expelled several Russian diplomats for whom, according to the authorities, there was evidence of direct involvement in activities that do not comply with international standards and generally accepted principles of conduct and work of diplomatic representatives. In terms of economy, the most recent and authentic example is perhaps the case from Veles, about the involvement of young Macedonian citizens and companies in disseminating information that allegedly had an impact on the US presidential elections in 2016. Although the young people were not the direct organisers, the weak regulations, and above all the shadow economy, were used and abused to push them into activities, for which they paid due taxes to the state, but caused an effect that had political repercussions. Regarding the information and communication sector, it is already widely known that the country, as well as many other countries in the region, is a victim of misinformation, which is mainly generated through Sputnik, in Serbia, where the information is downloaded and disseminated through local portals in the country. Another example is the involvement of foreign nationals in the events of 27 April 2017 in the Parliament of North Macedonia, where they tried together with domestic protesters to cause a crisis in the country. Namely, regardless of the level of involvement, even being physically present, they failed to cause destabilisation in order for the Agreement with Greece not to be signed.

Planned and Undertaken Counter-Measures

North Macedonia, as a NATO member, has an obligation to prepare the institutions and enhance resilience to hybrid threats, and for that purpose, the *National Strategy for Building Resilience and Tackling Hybrid Threats* was adopted. Cooperation with NATO in the security sector is one of the key steps that are being undertaken in relation to this issue. What is of great help is also the fact that the Alliance asked North Macedonia to establish a team for countering hybrid threats, aiming to prepare media in the country to deter disinformation campaigns from Russia (Kamcev 2020). Furthermore, the Cybercrime and Digital Forensics Sector in the Ministry of Interior singles out the Distributed Denial of Service or DDoS attacks as the most common hybrid threats to institutions and individuals (Nikolovski 2020). In 2020, the Army of North Macedonia

took part, as an observer, in several online sessions of the international NATO 'Cyber Coalition 2020', which encompasses defence from malware and hybrid challenges, and ever since 2021 has an active role in tackling hybrid threats.

Case Study: Bosnia and Herzegovina

Just as in the previous two cases, the main research subject deals with the analysis of hybrid threats in Bosnia and Herzegovina through several sections: Official Acknowledgement of Hybrid Threats; Potential Hybrid Threat; Activities that may be Related to Hybrid Threats; and Planned and Undertaken Counter--Measures.

Official Acknowledgement of Hybrid Threats

This subsection should present a set of hybrid threats that are recognised or qualified by official state institutions. However, the analysis shows that Bosnia and Herzegovina (B & H), although an aspirant for EU and NATO membership, currently neither has a publicly available document dealing with hybrid threats, nor a comprehensive strategic approach to address hybrid threats. In this regard, it is impossible to review or present official documents and sources. However, in 2019 only, as a member of international organisations and international commitments, with the aim of establishing certain strategic and normative frameworks, B & H proceeded to drafting the Guidelines for a Strategic Cyber-security Framework in Bosnia and Herzegovina (OSCE, 2019), with the help of the OSCE Mission to B & H. However, this document does not mention or analyse hybrid threats or hybrid dangers to B & H. The lack of political will to establish a strategic and normative framework for combating hybrid threats is clearly visible in the European Commission's Report on Bosnia and Herzegovina for 2021, stating: 'On hybrid threats, the EU has offered Bosnia and Herzegovina a research on hybrid risks in order to identify key weaknesses, which would be addressed through EU assistance. To date, the authorities have not expressed interest in participating in the research' (European Commission 2021: 113).

Potential Hybrid Threats

Although in recent years there has been some academic agreement that Bosnia and Herzegovina is exposed to hybrid threats, this analysis shows a deficit of professional and (academic) scientific identification/literature on potential hybrid threats to Bosnia and Herzegovina. In this regard, our main sources rely on individual and specific international studies that provide insight into potential hybrid threats. Therefore, Kico and Kapetanović (2019: 87) believe that 'almost all forms and aspects of social life, constitutional order, institutions of political, economic, judicial and security systems, as well as institutions of

religious, national, linguistic, educational and other forms cultural identity of citizens and of the constituent peoples of Bosnia and Herzegovina are targets of hybrid activities in B & H.' On the other hand, certain indexes place Bosnia and Herzegovina among the most vulnerable countries in terms of potential hybrid threats due to 'the political, social and economic environment of the country... which incites confusion over the country's strategic orientation' (NATO StratCom 2020: 3). We also find a practical example in the study 'War in Ukraine and the Western Balkans', where the authors state that the hybrid war, i.e. its consequences, are visible in the communication and information domain of the so-called 'cooked societies', which 'implies taking control over the target's contemplation and decision-making processes. When you take control over a target's strategy, then you take control of his decision-making process. The opponent is put in a situation to make decisions that benefit you, and are harmful for him' (Kico et al. 2022: 23).

Activities that may be Related to Hybrid Threats

Due to certain internal political and security specifics and backward animosities, Bosnia and Herzegovina is exposed to certain hybrid threats. We can take as an example the use of public diplomatic tools and media space to spread hybrid threats, which has intensified in recent years. Among the main goals of these activities are the paralysis of sovereignty and stopping the path towards the EU and NATO, as in a recent statement by Russian Ambassador Kalabukhov, who said that 'Russia will react in case of B & H's NATO membership' (Hina 2022). Moreover, mass disinformation campaigns against NATO and EU integrations are visible through social media and the internet, i.e. its content (e.g. Portal Sputnik, phrase 'Russian World', etc.), in order to control or change the political, security and social narrative. On the other hand, an example is the cultural 'offensive', which is visible through public gatherings and promotion of Russian interests by the organisation 'Night Wolves', as well as the drawing of certain murals with the symbol 'Z', anti-EU and anti-NATO propaganda, etc. Viewed from internal perspectives there are destabilising efforts that constantly generate complex and multi-dimensional threats. Therefore, the analyst Karup Druško (2021) detects complex methods of hybrid policy reflected in the activities of the Serb member of the Presidency of B & H, Milorad Dodik, who 'denies everything that is state, publicly stating that he harmonizes his views with Serbian foreign policy, at the same time repeatedly demanding secession, peaceful separation and the unification of Republika Srpska with Serbia, which can be more or less connected with Russian and pro-Russian activities in the Western Balkans'.

Planned and Undertaken Counter-Measures

This section should offer the development of Bosnia and Herzegovina's institutional capacity to counter all forms of hybrid threats, but due to the lack of an institutional-strategic framework, it is difficult to provide an overview of future activities and their capacities. However, in recent years there has been some interest, and also international assistance, to launch a unified approach to the development of basic strategic documents that would cover the area of hybrid threats. Following this, a series of workshops and exercises were held to strengthen the capacity of the state of Bosnia and Herzegovina in countering hybrid threats, especially cyberattacks. For example, based on the *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Threats Emanating from Cyberspace*, OSCE organised an exercise to assess the risk, level of readiness and protection of critical energy infrastructure for public and private institutions in B & H from terrorist attacks, with a focus on threats coming from cyber space (OSCE, 2013). Most experts agree that Bosnia and Herzegovina is one of the most vulnerable countries in terms of hybrid threats in the region, and the lack of an institutional and strategic framework makes it even more vulnerable. In this regard, future planned counter-measures are reflected in the urgent adoption of necessary legal and other norms that will create national and international conditions for a greater degree of resilience and adaptation to Euro-Atlantic integrations.

Discussion

This part of the research is dedicated to the comparison of previous findings from the individual researches of each of the three countries (Croatia, North Macedonia, and Bosnia and Herzegovina), taking into account the categories by which the analysis was done.

Table: Comparison of the of hybrid threats in Croatia, North Macedonia, and Bosnia and Herzegovina

	Croatia	North Macedonia	Bosnia and Herzegovina
Official Acknowledgement of Hybrid Threats	Yes	Yes	No
Potential Hybrid Threats	Yes	Yes	Yes
Activities that may be Related to Hybrid Threats	Yes	Yes	Yes
Planned and Undertaken Counter-Measures	Yes	Yes	No

The comparison of the research results shows that in all four categories of analysis (Official Acknowledgement of Hybrid Threats; Potential Hybrid Threats; Activities that may be Related to Hybrid Threats; Planned and Undertaken Counter-Measures) there are certain activities in the three analysed countries, even though the content and actors involved are different.

In the case of Croatia, there are the most elements that indicate that state institutions not only recognise the exposure to hybrid threats, but also specify them by topic and hybrid actors. While in North Macedonia, in official documents, it is stated that the country is exposed to hybrid threats, but it is not specified which exactly and from which hybrid actor the greatest threat is. Meanwhile, the activity of international organisations is noticeable in Bosnia and Herzegovina, which instruct state institutions that it is necessary to start dealing with this area, where they offer them help and support, but without an adequate response from the other side. More forward, in the case of all three countries, there are recognised – primarily in the academic world – potential hybrid threats, and activities that may be related to hybrid threats which have not been confirmed by state institutions, but can certainly be very relevant for the discussion of whether in reality they represent hybrid threats, a danger of some other nature or whether they should be rejected from the discussion. As far as planned and undertaken hybrid counter-measures are concerned, the comparative analysis shows that Croatia implements the most concrete measures at the level of the three compared countries. North Macedonia also tries to implement a certain number of measures, while we note the complete absence of official measures that would be publicly available and visible in the case of Bosnia and Herzegovina.

Conclusion

All countries worldwide are more or less exposed to different forms, dynamics and strengths of hybrid threats. The three analysed countries are not excluded: Croatia, North Macedonia, and Bosnia and Herzegovina. The analysis showed that all three countries are exposed to hybrid threats. Official documents have confirmed that Croatia is exposed to the following hybrid threats: defamatory campaigns; elements of non-conventional, asymmetric, and cyber actions; intelligence and hybrid operations in the economic sphere; foreign intelligence activities; and 'fake news' campaigns. For North Macedonia, official documents noted that the country is exposed to various forms of hybrid threats, but which one is not specified. In the case of Bosnia and Herzegovina, there are no official positions of the competent institutions regarding the exposure to hybrid threats; the interviewed experts working in the institutions responsible for the implementation of security activities stated that the state is exposed to such threats. In order to supplement this insight, for all three countries we analysed

the available academic and professional literature sources from international as well as Croatian, Macedonian and B & H experts. All sources consulted agree that all three countries are exposed to different forms of hybrid threats to a greater extent than stated in official documents.

The answers to the part of the research question about how they deal with hybrid threats are different. Croatia and North Macedonia are developing and publishing documents discussing hybrid threats and how the state should deal with them. It is noticeable that Croatia is more focused and direct than North Macedonia. That should be attributed to longer tenure in NATO and full membership in the European Union. This is relevant because under the influence of discussions and activities in these organisations, states have the opportunity to exchange views, learn, upgrade the existing corpus of knowledge and skills, and develop new mechanisms. So, although this was not the interest of the research, the positive significance and impact that full membership in the EU and NATO gives to each member state can be confirmed. As far as Bosnia and Herzegovina is concerned, unfortunately, there was no official activity in the form of publicly available information related to the activities of the competent institutions in this area. Despite this, it is clear that there is no political will to establish a strategic and normative framework for combating hybrid threats.

Regarding the discussion of counter-hybrid solutions that countries are developing, yet again the solutions found are very different. For the cases of Croatia and North Macedonia, we can point out that they actively participate in exercises organised by the organisation to which they have access – both participate in NATO exercises, and Croatia also participates in EU exercises. In this way, they learn and hone their skills, abilities and capabilities. In addition, Croatia is a member of the European Center of Excellence for Countering Hybrid Threats, and has recently established the Security and Intelligence Agency Center for Cyber Security, which, among other tasks, deals with hybrid threats coming from cyberspace. For Bosnia and Herzegovina, we must emphasise once again that there are no developed counter-hybrid solutions and most likely there are no solutions which are in the development phase.

In conclusion, the analysis showed that all three countries are exposed to different forms of hybrid threats, they treat them differently and have different approaches to developing counter-hybrid solutions. The most significant number of activities was recorded in the case of Croatia, followed by North Macedonia, while in the case of Bosnia and Herzegovina, according to publicly available sources, there are no significant activities in this area. With that, the central research question of this paper is answered. In addition to its primary purpose, the research is additionally significant because it compared the activities and solutions of the three countries that were part of a larger political entity until 30 years ago (all three were socialist Republics in the former Yugoslavia) and showed that the country's stability, built and functional state institutions,

membership in international organisations (with some additional factors) are significant prerequisites for dealing with hybrid threats. Also, the research highlighted certain well-known points, such as facing any security challenge requires a lot of effort and joint work of many actors in each society, so this paper may encourage some of them to engage in more activities. In addition, it is essential to provide other researchers of these and similar topics worldwide, with the opportunity to see the state of affairs in small countries with limited resources, what solutions they approach and how they achieve them or not.

References

Akrap, Gordan (2019): Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura. *Strategos* 3(2), 2019: 37–49.

BalkanInsight (2018): Russian Threat in Montenegro was Severe: available at https://balkaninsight.com/2018/07/04/russian-threat-in-montenegro-was-severe-report-07-04-2018/ (15 May 2022).

Brzica, Nikola (2019): Hibridno ratovanje i suvremeni sukobi, Doctoral thesis, University of Zagreb, The Faculty of Political Science: available at https://repozitorij.fpzg.unizg.hr/islandora/object/fpzg:863 (18 May 2022).

Burnham, Peter; Gilland, Karin; Grant, Wyn; Layton-Henry, Zig (2006 [2004]): Research Methods in Politics, New York: Palgrave Macmillan.

Cattler, David (2021): What is NATO doing to address hybrid threats? available at https://www.nato.int/cps/en/natohq/news_183004.htm (12 May 2022).

Croatian Parliament (2017): National Security Strategy of the Republic of Croatia. available at https://www.morh.hr/wp-content/uploads/2018/04/strategy_18012018.pdf (21 May 2022).

Cvrtila, Željko (2017): Hibridni rat – suvremeni naziv za već poznate oblike ratovanja. *Journal Zaštita*, 12 (2017): 14–17.

Devine, Fiona (2005 [2002]): Qualitative methods, in: Marsh, David and Stoker, Gerry (ed.) (2005), Teorije i metode političke znanosti, Zagreb: Fakultet političkih znanosti (In the original: Theory and Methods in Political Science (2002), New York: Palgrave Macmillan), 191–209.

European Centre of Excellence for Countering Hybrid Threats (2022): Hybrid threats as a concept. available at https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (12 May 2022).

European Commission (2022a): Hybrid Threats. available at: https://ec.europa.eu/defence-industry-space/eu-defence-industry/hybrid-threats_en (12 May 2022).

European Commission (2022b): Western Balkans. available at https://ec.europa.eu/info/research-and-innovation/strategy/strategy-2020-2024/europe-world/international-cooperation/western-balkans_en (13 May 2022).

European Commission (2021): Report on Bosnia and Herzegovina for 2021. available at https://europa.ba/wp-content/uploads/2021/10/izvjestaj-o-bosni-i-hercegovini-za-2021-godinu_1636467943.pdf (24 May 2022).

Falon, Isabelle; Mazzucchi, Nicolas; Patry, Jean-Jacques (2018): Countering hybrid threats: EU and the Western Balkans case. Directorate General for External Policies of the Union and European Parliament. available at https://www.europarl.europa.eu/RegData/etudes/STUD/2018/603851/EXPO_STU(2018)603851_EN.pdf (15 May 2022).

Government of the Republic of North Macedonia (2021): The Strategy for Building Resilience and Tackling Hybrid Threats. available at https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf (29 May 2022).

Greene, Samuel; Asmolov, Gregory; Fagan, Adam; Fridman, Ofer; Gjuzelov, Borjan (2020): Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them. Directorate General for External Policies of the Union and European Parliament. available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653621/EXPO_STU(2020)653621_EN.pdf (15 May 2022).

Guardian (2016): Montenegrin prosecutor says Russian nationalists behind alleged coup plot. available at https://www.theguardian.com/world/2016/nov/06/montenegro-prosecutor-milivoje-katnic-russian-nationalists-behind-alleged-coup-plot (15 May 2022).

Harding, Luke; Belford, Aubrey; Cvetkovska, Saska (2017): Russia actively stoking discord in Macedonia since 2008, intel files say. The Guardian. available at: 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 (15 May 2022).

Hina (2022): Russian ambassador: BiH can join NATO, but Moscow will react to threat. N1 multimedia information platform. available at: https://ba.n1info.com/english/news/russian-ambassador-bih-can-join-nato-but-moscow-will-react-to-threat/ (25 May 2022).

Hopkins, Valerie (2017): Indictment tells murky Montenegrin coup tale. Politico. available at: https://www.politico.eu/article/montenegro-nato-milo-dukanovicmurky-coup-plot/ (15 May 2022).

Ilievski, Hristijan (2022): Како Македонија да стане поотпорна кон хибридните закани? *Prespublika*: available at http://respublica.edu.mk/blog/politika/kako-makedonija-da-stane-pootporna-kon-hibridnite-zakani/ (29 May 2022).

Kamcev, Boris (2020): NATO is forming a team to combat hybrid threats in North Macedonia, Media Information Agency. available at: https://mia.mk/hachinson-nato-formira-tim-za-borba-so-hibridni-zakani-vo-severna-makedoni-a/ (30 May 2022).

Karup Druško, Dženana (2021): Nova generacija ruskog ratovanja je bez ispaljenog metka osvojila strateški važna uporišta na Balkanu). available at: https://avangarda.ba/post/type-1/965/Nova_generacija_ruskog_ratovanja_je_bez_ispaljenog_metka_osvojila_strateski_vazna_uporista_na_Balkanu (31 May 2022).

Kico, Ahmed; Kapetanović, Miralem; Šušnica Srđan (2022): Rat u Ukrajini i Zapadni Balkan. available at https://atlantskainicijativa.org/wp-content/uploads/2022/04/RAT-U-UKRAJINI--I-ZAPADNI-BALKAN.pdf (26 May 2022).

Kico, Ahmed; Kapetanović, Miralem (2019): Bosna i Hercegovina i Zapadni Balkan: Aspekti geopolitike i hibridnog rata), Sarajevo: Atlantska inicijativa.

Ministry of Defense of the Republic of North Macedonia (2020): Defence Strategy of the Republic of North Macedonia, Official Gazette no.75/24/03/2020. available at https://www.mod.gov.mk/storage/2021/06/Defence-Strategy-of-the-Republic-of-North-Macedonia.pdf (25 May 2022).

Mitrović, Miroslav (2018): The Balkans and Non-Military Security Threats – Quality Comparative Analyses of Resilience Capabilities Regarding Hybrid Threats. *Security and Defence Quarterly* 2018; 22(5), 20–45. available at: https://securityanddefence.pl/pdf-103314-36188?filename=The%20Balkans%20and.pdf (14 May 2022).

NATO Parliamentary Assembly (2018): Security in the Western Balkans. available at: https://www.nato-pa.int/download-file?filename=/sites/default/files/2018-12/178%20PCNP%2018%20E%20rev.1%20fin%20-%20SECURITY%20IN%20THE%20WESTERN%20BALKANS%20-%20ANDREYCHUK%20REPORT.pdf (13 May 2022).

NATO Strategic Communications Centre of Excellence (2020): Risks and Vulnerabilities in the Western Balkans. available at https://stratcomcoe.org/publications/risks-and-vulnerabilities--in-the-western-balkans/57 (14 May 2022).

NATO StratCom (2020): Russia's Footprint in the Western Balkan Information Environment (Summary). Riga: NATO Strategic Communications Centre of Excellence. available at: https://stratcomcoe.org/publications/russias-footprint-in-the-western-balkan-information-environment--summary/51 (27 May 2022).

Nikolovski, Marjan (2020): Хибридните закани како нова форма на закана за демократијата), *Prespublika*. available at https://znm.org.mk/хибридните (27 May 2022).

Organization for Security and Co-operation in Europe (2019): Guidelines for a strategic Cybersecurity Framework in Bosnia and Herzegovina. available at https://www.osce.org/mission--to-bosnia-and-herzegovina/438383 (25 May 2022).

Organization for Security and Co-operation in Europe (2013): Good Practices Guide on non--Nuclear Critical Energy Infrastructure Protection from Threats Emanating from Cyberspace. available at: https://www.osce.org/files/f/documents/4/b/103500.pdf#_blank (01 Jun 2022).

Rrustemi, Arlinda; de Wijk, Rob; Dunlop, Connor; Perovska, Jovana; Palushi, Lirije (2019): Geopolitical Influences of External Powers in the Western Balkans. Hague Centre for Strategic Studies.

Rühleu, Michael (2021): The Nine Commandments on Countering Hybrid Threats. *Internationale Politik Quarterly*. available at: https://ip-quarterly.com/en/nine-commandments-countering--hybrid-threats (13 May 2022).

Security and Intelligence Agency of the Republic of Croatia (2021): Public Report 2020/21: available at Public-Report-2020-en.pdf (soa.hr) (21 May 2022).

Security and Intelligence Agency of the Republic of Croatia (2017): Public Report 2017: available at: https://www.soa.hr/files/file/SOA-Public-Report-2017.pdf (21 May 2022).

Šoštarić, Tomislav (2019): Hrvatska i Slovenija na meti mađarskih i talijanskih teritorijalnih frustracija*). Al Jazerra web portal*: available at https://balkans.aljazeera.net/teme/2019/6/15/hrvatska-i-slovenija-na-meti-madarskih-i-talijanskih-teritorijalnih-frustracija (21 May 2022).

Think Tank of the European Parliament (2015): Understanding hybrid threats. available at https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/ (13 May 2022).

Veljković, Sandra (2019): Novi incident: Vijećnik objavio kartu Italije kojoj je pripojio hrvatsku obalu, *Večerni List web portal:* available at https://www.vecernji.hr/vijesti/novi-incident--vijecnik-objavio-kartu-italije-kojoj-je-pripojio-hrvatsku-obalu-1323699 (21 May 2022).

Warsaw Institute (2019): Russia's Hybrid Warfare in the Western Balkans: available at: https://warsawinstitute.org/wp-content/uploads/2019/03/Russias-Hybrid-Warfare-in-the-Western--Balkans-Warsaw-Institute-Special-Report.pdf (15 May 2022).

Wikipedia (2022): Southeast Europe. available at: https://en.wikipedia.org/wiki/Southeast_Europe (13 May 2022).

Yin, K. Robert (2007 [2003]): Studija slučaja: Dizajn i metode, Zagreb: Fakultet političkih znanosti (In the original: Case study research: Design and methods, London: Sage Publication).

Robert Mikac *(corresponding author) is Associate Professor at the Faculty of Political Science of the University of Zagreb. The areas of his interest and expertise are: International Relations; International and National Security; Security Management; Crisis and Disaster Management; Civil Protection; Afghanistan; Privatization of Security; Critical Infrastructure Protection and Resilience; and Migrations and Security. He is the author and co-author of six books and more than forty scientific articles. Prior to his academic career, he served in various positions within the Croatian security sector from the operational to the strategic level in the country and internationally. Among other things, he served in the NATO ISAF mission in Afghanistan. For his merit in Afghanistan, he was awarded with the NATO Medal and the Order of Merit of the Italian Republic. Email: robert.mikac@yahoo.com*

Marina Mitrevska *is Full Professor at the Institute for Security, Defence and Peace at the Faculty of Philosophy, University of Ss. Cyril and Methodious in Skopje, Republic of North Macedonia. She is the Head of the third cycle of doctoral studies in security, defence and peace. She is a member of the Accreditation and Evaluation Board of Higher Education in the Republic of North Macedonia. She is Editor-in--Chief of the international scientific journal Contemporary Macedonian Defence. Her field of scientific research is security, diplomacy, peacekeeping operations and crisis management. She is actively engaged in researching and publishing scientific papers and books in the field of security. She is the author of eleven books and more than a hundred scientific papers. Email: marinamitrevska@yahoo.com*

Mirza Smajić *is Associate Professor at the Faculty of Political Science in Sarajevo. His research interests include security studies, human security, national security and law enforcement and police studies. As an author or co-author, he has published four books and studies, and a number of professional and scholarly papers published in Bosnia and Herzegovina and abroad. He has participated as a researcher or consultant in a large number of congresses and projects in Bosnia and Herzegovina, Serbia, and Croatia. Email: mirza.smajic@fpn.unsa.ba*