DOI: 10.53477/2668-2001-21-14

ASYMMETRIC OPERATIONS OF THE HOSTILE MILITARY INTELLIGENCE SERVICES ON THE ALLIED STATES TERRITORIES

Robert Călinoiu[1]
"Carol I" National Defence University
Dănuț Chiriac
Hyperion University, Bucharest, Romania

Abstract

Globalization and technological developments brought to societies huge benefits, but also new security challenges. State or private entities, having access to new, advanced technologies, and benefiting of the rapid and free movement, developed methods and strategies to harm their perceived enemies. National security, considered alone or in conjunction with those of the allied states or within the security organizations is challenged lately by hostile acts performed by various entities, aimed at weakening societies, value systems, beliefs or even the simply well-being of the citizens. Intelligence services, as part of the national / organizational security systems are called to discover, perform early warning, monitor, and counter such aggressive actions, even if a clearly attribution of the perpetrator is difficult. Our endeavour is to draw a picture of the current preoccupations in the field, presenting also three cases where the uncertainty of the transgressors has been eliminated without any shadow of doubt.

Keywords: asymmetric; hybrid; threats; intelligence; hostile; strategy; security; case study.

INTRODUCTION

The period of the years 2000 has been characterized by an accelerated globalization, possible due to the freedom of movement of citizens and goods that followed the opening of the borders in large parts of the World. This freedom was accompanied by the huge technological progress leading to major breakthroughs in the field of communications and permitting an easy access to information.

The 2003 EU Security Strategy (EUSS) described very well the situation of that period on the European continent, mentioning the challenges to the European and international security, listing terrorism, illegal proliferation of the weapons of mass destruction, regional conflicts, failed states and organized crime.

Furthermore, it correctly envisioned the fact that, in the globalization era, the threats apparently situated at distance represent a concern as big as threats situated in its proximity, reality requiring the developing of a security culture allowing a prompt reaction, when necessary, in defending the strategic objectives of the EU (Council of the European Union 8.12.2003)[2].

Despite the accuracy in describing the threats, part of these have been affected the EU security sooner than expected. Starting 2004, a string of terrorist attacks took place in Western Europe, characterized by a big number of casualties and followed by political decisions and societal trends with a significant impact on the European security. Question marks on the existing alliances viability aroused, followed by doubts on the political and economic agreements. Populist leaders took the power and partisans of restricting the freedom of movements and other collective rights have emerged.

[1] Corresponding author: robert.calinoiu@eeas.europa.eu
[2] "*In an era of globalization, distant threats may be as much a concern as those that are near at hand... The first line of defense will be often be abroad. The new threats are dynamic...Conflict prevention and threat prevention cannot start too early*".

The aforementioned challenges permitted to hostile intelligence services to exploit the vulnerabilities by encouraging the separatists' movements in different countries, with some painful successes. Their actions were also possible due to the technological developments, combined with the rights given by the continuous openness of the World. However, despite the asymmetric approach and the covert nature of operations, the technology also permitted the attribution of some cases to their real perpetrators, eventually acting appropriately to impede the repetition.

METHODOLOGY

Our approach in addressing the subject is a four-step one. First, we will try clarifying the main terms used, namely asymmetric threats and hybrid threats.

The second step is presenting the efforts done at national level, the North Atlantic Treaty Organization (NATO) level, the European Union (EU) level, and joint level in countering the hybrid (asymmetric included) threats.

Finally yet most importantly and in deeper length, we will be presenting few asymmetric operations perpetrated by hostile military intelligence services on the territories of the EU, NATO or allied countries.

Based on the case studies presented, we will draw some conclusions concerning the effectiveness of the efforts of countering the asymmetric / hybrid threats to the security interests at the national and allied levels.

DEFINING THE TERMS

In order to define the main terms, ***asymmetric threats*** and ***hybrid threats***, we are referring to three sources belonging to the two most relevant organizations for Romania's security point of view, NATO and EU, and national ones. As such, the first definition comes from the **NATO** Glossary of Terms and Definitions (NATO Standardization Office - NSO 2019), according to which the ***asymmetric threat*** is "*A threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain a disproportionate result*". In order to further clarify our approach in the field, we are also adding the definition of the ***hybrid threat***, from the same source, which is "*A hybrid threat is a type of threat that combines conventional, irregular and asymmetric activities in time and space"*. These two combined explains why usually the asymmetric threat is addressed by many in conjunction with the other two, conventional and irregular, under the umbrella of the hybrid concept.

The second definition we would like to present is deriving from **EU** documents (Daniel Fiott 2019), where the ***asymmetric threats*** are "*Tactics and strategies that are designed to exploit weaknesses and vulnerabilities in powerful military and political actors*". Furthermore, the EU (European Parliament; European Commission 2016) considers that "***Hybrid threats*** *can be characterized as a mixture of coercive and subversive activity, conventional and unconventional methods which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of open organized hostilities*".

On the same subject, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), defines this type of threat as "*…an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means*". (European Centre of Excellence for Countering Hybrid Threats 2021)

At the **national** level, the ***asymmetric threat*** is defined within the Guide of the National Defence Strategy for 2015 – 2019 (Romanian Presidency 2015), as "*The threat emanating from a non-state actor employing unconventional methods and means in order to provoke important damages compared to the level of actions, by exploiting states vulnerabilities and avoiding a direct military confrontation*". Furthermore, the ***hybrid threat*** is defined as "*The threat emanating from a state or non-state actor utilizing a variety of methods and means, conventional and unconventional (political, military, diplomatic, economical, cyber, informational), together or separated, in order to fulfil its goals*".

In analysing the two national definitions we should take into consideration that the separation state/non-state actors made in 2015 is no longer valid, according to the current NATO and EU documents adopted with Romania's agreement as a voting member.

COUNTERING THE ASYMMETRIC / HYBRID THREATS

Countering Asymmetric / Hybrid Threats at the National Level

At the national level, the National Strategy for State Defense 2020-2024 (NSSD 20-24) (Presidential Administration 2020) foresees from the cover motto the need to overcome the different challenges ahead. In the foreword, NSSD 20-24 connects from the very beginning the national security to the security of NATO and EU, acknowledging the complex links among the three notions and the common goals. Later on, other strategic partners are associated to the national security, like United States of America (USA), and specific policies and actions at national and international levels.

Flexibility, adaptability, and rapid reaction on crises are the main features of the national strategic leadership, allowing anticipation and planning in order to avoid the strategic surprise. The technological developments are acknowledge for their potential contribution to the raise of the complexity of the risks and threats to the national security. Asymmetric and cyber-attacks, disinformation, fake news, use of civil technologies in asymmetric and hybrid actions should constitute a constant preoccupation for the national security services.

The Greater Black Sea Area security concerns also deeply the national security through the vectors of instability situated in this region. Protracted conflicts, immigration, changes of the borders by force, the use of the asymmetric and hybrid tactics and means to promote security goals, originated from the area, are all issues affecting our security and our allied and partners' - like Republic of Moldova's security.

The Strategy takes into discussion other threats like the reconfigurations of the relations among global actors, the aggressive posture of the Russian Federation towards Western and NATO states materialized in frequent breaches of the international laws, the assertiveness of regional state having global ambitions, migratory flows, and COVID-19 pandemic challenges. A special paragraph is dedicated to the diversification of the asymmetric, cyber and hybrid threats of hostile entities, and another one to the possible threats emerging from the misuse of the technological developments (artificial intelligence, machine learning, dark web, cloud and smart computing, big data, internet of things, fast internet/5G, ransomware, hacktivism, unmanned systems). In the abovementioned stances, specific security actions being required from the state organizations.

NSSD 20-24 foresees also the need to develop mechanisms for citizens to understand, prevent and react when confronting threats, risks and vulnerabilities (Presidential Administration 2020). In this respect, according to one of the projects of the Presidency, a culture specific to the security domain has to be developed.

Based on the NSSD 20-24, the White Book of Defense 2020 (WB 20) (Ministry of National Defense 2020) is meant to implement the provisions of the aforementioned document in practice at the Ministry of National Defense (MoND) level. WB 20 observes that the determinations of reconfiguring the World's power centers and the low appetite for a conventional major conflict amplify the asymmetric and hybrid actions to fulfill the strategic goals for state actors.

In order to counter the threats, the Ministry of National Defense intends to develop strong, credible, interoperable, flexible and efficient defense capabilities, having especially in mind the asymmetric and hybrid challenges.

Integrating the new technologies in the daily work, digitalization, modern command and control systems are objectives of immediate interest. The defense organization is tasked to adapt in order to counter the new disruptive technologies, the threats in the cyber environment, and the disinformation and hostile propaganda activities.

Being member of a complex security architecture at the NATO at EU levels, MoND participates in NATO projects like Strategic Air Capability, NATO Airborne Early Warning & Control, Air Command and Control System, or EU projects as European Defense Fund, European Defense

Industrial Development Program, Coordinated Annual Review on Defense, and Permanent Structured Cooperation and some of its subsequent projects.

Countering Asymmetric / Hybrid Threats at the NATO Level

NATO is focusing on addressing the overall hybrid threats, its documents using this formula and not asymmetric threats in particular. By hybrid, the Alliance is referring to propaganda, deception, sabotage, disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and other non-military tactics used by adversaries to destabilize the security in areas of interest and spreading uncertainty within the populations.

NATO's Secretary General Jens Stoltenberg considers (Finland, 2 October 2017) that the late characteristics of the attacks are the higher pace and strength, enabled by the technological developments.

Alliance's strategy in fighting hybrid or classical actions foresees that the main obligation to counter them belongs to the member states (MS), NATO standing ready to offer support according to Article 5 provisions (NATO 2019). In this respect, in 2018 NATO member states representatives decided to to create counter-hybrid support teams, charged with offering expertise to MS if demanded. Moreover, since the reorganization of the Intelligence structures in NATO, the newly created Joint Intelligence and Security Division developed a hybrid analysis structure responsible for tailored warnings.

Taking into consideration the global character of the hybrid threats, NATO is also consolidating its partnerships with third states and like-minded organizations. A proof of the NATO – EU solid partnership in countering hybrid threats is demonstrated by the inauguration (October 2017), of the European Centre of Excellence for Countering Hybrid Threats based in Helsinki by the Secretary General Jens Stoltenberg and the High Representative and Vice President of the European Commission, Federica Mogherini (NATO 2017). The Center functions as a fusion structure of knowledge, supporting member states in refining their capabilities to fight the hybrid threats.

Countering Asymmetric / Hybrid Threats at the EU Level

European Union has been preoccupied by the asymmetric threats since its first security strategy, in 2003. At that time, the Union faced a variety of dangers there were not purely military, and consequently could not be addressed by military means. Countering proliferation of weaponry and dual use technology, terrorism, illegal migration, organized crime, disinformation, propaganda, required a mixture of instruments not all available and efficiently coordinated.

Over the time, the threats have diversified exponentially, and so the preoccupations at the EU level. Starting 2016, the European Union has established a variety of processes in various policy fields through specific documents ("2016 Joint Framework on countering hybrid threats – a European Union response"; "2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats").

The results of these processes have been included in the Progress Reports to the Council in the next three years. The execution of the 2016 Joint Framework and the 2018 Joint Communication's provisions has been advanced by cooperation among the MSs, EU bodies, and international allies (European Commission 2020).

The EU has been continuously adjusting to the shifting security challenges of the hybrid domain: refining policies, updating processes and procedures, anticipating trends and evolving threats. As such, the MSs established in July 2019 a "Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats", having as a central goal to support the specific cooperation among members, with a particular accent on fighting disinformation.

The COVID-19 pandemic brought a new array of challenges, as it is obviously used by some state players to create societal rifts in foreign countries, blur the responsibilities, manipulate the vulnerable public opinion and advance their goals through the newly discovered *medical diplomacy*, namely providing vaccines to some friendly member states from alliances or organizations of interest in exchange for promoting their policies in strategic fields of interest. This type of action, certainly

hybrid in nature, is part of the same strategy of divide and conquer very effective in other cases like BREXIT.

In order to better analyses and counter the hybrid threats, within the EU Intelligence and Situation Centre (EU INTCEN) has been established in 2016 the EU Hybrid Fusion Cell (HFC) (EU Military Staff 2019), having the role of coordinating the domain within EU intelligence bodies. The HFC performs all-source study of hybrid and cyber threats together with the Intelligence Directorate of the EU Military Staff (EUMSINT), within the format of the Single Intelligence Analysis Capacity (SIAC), and provide written intelligence products or oral briefs as required by the stakeholders.

Another step towards addressing the hybrid threats has been the creation of the European Centre of Excellence for Countering Hybrid Threats (CoE), in 2017, by nine countries, NATO and EU. As of today, Helsinki CoE has 27 members, bringing together their knowledge and offering their fusion expertise in the field of interest.

ASYMMETRIC OPERATIONS PERPETRATED BY HOSTILE MILITARY INTELLIGENCE SERVICES ON THE TERRITORIES OF THE EU AND/OR NATO COUNTRIES

In line with the main goal of this paper, we would like to present a few case studies on asymmetric operations perpetrated by hostile, assertive military intelligence services in order to better understand the modus operandi and draw possible useful conclusions on specific early warning and countering actions.

The focus will be on the Russian military intelligence service (Glavnoye razvedyvatel'noye upravleniye – GRU), involved in the last years on an array of asymmetric hostile operations. These were ranging from poisoning political opponents of the regime abroad or inland (Alexander Litvinenko, Serghei Skripal, Alexander Navalnii), attempts of overthrowing democratic regimes (Republic of Montenegro), meddling in the democratic elections in foreign countries (United States, Germany) or referendums (UK), discrediting efforts of anti-doping sport association (The Netherlands).

Unfortunately, even if perceived as acts of war by some leaders, these operations are difficult to attribute and do not fall into the UN Charter definition of acts of war[3]. Consequently, and due to the different respect paid to the international laws by democratic countries, they cannot be answered proportionally, leaving the options to diplomatic expulsions, economic sanctions, and blaming speeches during the international conferences or official meetings.

Case study concerning the Russian military intelligence service operation to sabotage and delegitimize The World Anti-Doping Agency – WADA's activity

This case study is relevant due to its target situated outside of the usual range of military or political targets of a military intelligence service, the vast amount of resources involved, and the irony on acting against an environment where fair play is supposed be the norm.

The objective is the World Anti-Doping Agency – WADA, based in The Hague, and the efforts were directed to sabotage and make irrelevant the investigation of WADA against the doping program of the Russian athletes. However, the operation involved few teams acting on at least four continents (Europe, South America, North America, and Asia), inferring that, if in a case apparently outside the main scope of a military organization are used so many resources, in an operation falling under the regular portfolio of missions, the resources would be unrestrained.

On 4 October 2018, the US Department of Justice (DoJ) made public (US Department of Justice 2018) the indictment of a group of seven Russian GRU officers, accused of five crimes under the U.S. Law. The indictment shows that from about December 2014 and lasting until at least May 2018, the perpetrators hacked computers belonging to U.S. citizens, companies, international organizations, and their respective personnel situated round the world, based on their strategic interest to the Russian government.

[3] Article 51 of UN Charter states that "*Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations*."

The aims of the scheme was to make public the unlawful acquired data as part of an influence and disinformation campaign meant to "undermine, retaliate against, and otherwise delegitimize the efforts of international anti-doping organizations and officials who had publicly exposed a Russian state-sponsored athlete-doping program" (US Department of Justice 2018).

The prosecution alleges that the offenders, and unidentified plotters, using false characters and proxy servers, investigated targets, sent spear phishing messages, unlawfully collecting information.

When needed, GRU specialised personnel travelled on the globe where the persons of interest were actually situated. The Trojan horse used to access the information of interest was very often the Wi-Fi networks, either public or private, including the hotel ones. After acquiring the information, the deployed team sent it to its handlers in Russia for utilisation.

In July 2016, WADA's Independent Person Report was issued, showing Russia's methodical state-sponsored sabotage of the drug testing process prior to, during, and subsequent to the 2014 Sochi Winter Olympics. Soon after the publication of the report and the International Olympic Committee's and IPC's following resolutions concerning the elimination of Russian competitors, the plotters hacked the networks of WADA, the United States Anti-Doping Agency (USADA), and International Court of Arbitration for Sport (TAS/CAS). When needed, they travelled to Rio de Janeiro, Lausanne, or Ottawa, to perform hacking operations after obtaining the needed login credentials using the hotels Wi-Fi networks.

Starting September 2016, the plotters started releasing to the public and the media the stolen data, including information about athletes allowed to use prohibited substances due to personal health issues, in order to create a picture of a generalised use of forbidden medicines among the athletes. When better serving the goal, the information had been altered from its accurate form, 250 sportspersons from 30 states being exposed.

The media campaign lasted until the end of 2018, around 186 reporters being periodically contacted in an effort to magnify the fake revelations.

Case study concerning the Russian military intelligence service operation against the Organization for the Prohibition of Chemical Weapons (OPCW)

In April 2018, four defendants indicted in US in the WADA case, using diplomatic credentials, deployed to The Hague in the Netherlands to pursue a close access operation targeting the Organization for the Prohibition of Chemical Weapons (OPCW). As later documented, all four were GRU operatives, and their mission included later on a second stage trip to Spiez, Switzerland.

In Spiez, the object of interest was the Swiss Chemical Laboratory, an OPCW accredited facility specialised in analysing military chemical agents, including the substance that the United Kingdom authorities suspected it was used to poison a former GRU officer in that country, Serghei Skripal.

Figure 1. Group of Russian GRU officers at their arrival at Schiphol

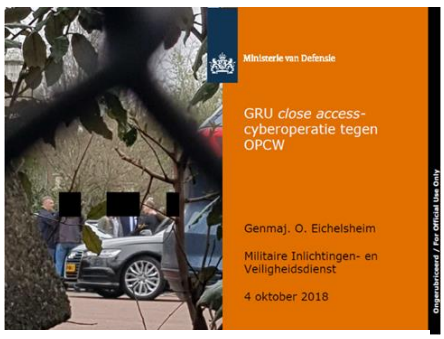

Figure 2. The cover of the Dutch Defense Intelligence Service Report

However, the team of four was discovered on the course of the OPCW intrusive mission by the Dutch defence intelligence service (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) (Ministerie van Defensie, Militaire Inlichtingen- en Veiligheidsdienst 2018). The MIVD counter-espionage action led to the capture of specialised Wi-Fi GRU gear unprofessionally placed in the trunk of a hire vehicle abandoned in the close proximity to the OPCW Headquarter.

After performing the specific checking, the Dutch MIVD discovered that the equipment has been used in various places around the globe, including Brazil, Switzerland and Malaysia.

The modus operandi being described in the previous case study, we would not insist on it, limiting the information to the essential part and looking to underline the outcome, the complete failure.

The success in disrupting the illegal Russian GRU officers had been possible due to the close cooperation of the intelligence services across the Atlantic, and due to the mistakes made by the operatives in the preparation of the mission and on the Netherlands territory. Analysing the facts, an astonishing conclusion surfaces: the Russian officers did not care much about the consequences of their illegal actions, either due to their self over confidence and disrespect towards local intelligence services, or the solid back up at home. Unlike in other situations, bearing diplomatic Russian passports did not offer to the authorities to possibility to deny their association with the Russian Government, unlike in other instances where private organizations, like Fancy Bears, where made responsible for the wrongdoings.

Case study concerning the Russian military intelligence service operation on the Republic of Montenegro territory

On 16 October 2016, day of Parliamentary elections in the Republic of Montenegro, a coup attempt took place in the Republic, having the ultimate goal of changing the power favourable to the accession of the country in NATO with another one opposing joining the Alliance and friendly to Russia.

However, due to a series of events, the coup had failed, and on 5 June 2017, Republic of Montenegro became the 29th member of NATO.

According to different sources (Stevo 2019), (Bajrovic Reuf 2018) citing the Montenegro judicial proceedings, on the eve of Montenegro's 2016 parliamentary elections, police in Podgorica etained former Serbian gendarmerie commander Bratislav Dikic and 19 other individuals on charges of forming a criminal organization with the intent to overthrow the government. Soon after, the Special Prosecutor for Organized Crime had indicted fourteen people in the capital city of Podgorica. These people were later identified as Russian agents, Serbian extremists, and leaders of the Montenegrin opposition alliance (Democratic Front – DF) prepared to oust the government violently on election night. According to officials, Serbian nationals initiated the enterprise in early 2016 under the direction of Russian GRU and Russian Federal Security Service (Federal'naya Sluzhba Bezopasnosti – FSB) operatives.

The planned takeover was relatively straightforward. Under the command of Bratislav Dikic, a group of 20 individuals dressed in stolen Montenegrin police uniforms was to occupy parliament on the night of the election. Meanwhile, the Democratic Front would declare victory and call on hundreds of mobilized supporters to storm the building. In response, the group of disguised police would fire on opposition protestors. The DF would then call for nationwide protests, alleging that the violence was an attempt to prevent the triumphant opposition from seizing the reins of government. The plotters also planned to assassinate the Prime Minister, Milo Djukanovic. In this manner, opposition leadership envisioned a state of emergency as the springboard to state control.

Montenegrin authorities, however, successfully prevented the coup attempt. On October 12, four days before the elections, former police officer Mirko Velimirovic confessed to his involvement as a gunrunner, giving the Montenegrin authorities their initial lead. Investigations ensued, leading to the discovery of encrypted phones among ten individuals, including leaders of the Democratic Front. Arrests commenced, and officials confiscated rifles, spiked road barriers, handcuffs, batons, and other equipment exclusive to the state's special police.

As detentions were underway, Montenegrin security services received communications from Serbia's Security Intelligence Agency (Besbednoso-Informativna Agencija – BIA) that 50 Russian GRU special forces troops had entered Montenegro's mountainous Zlatibor region from Serbia on the night of 15 October. Their aim was first to neutralize a nearby Montenegrin special forces camp and then to travel to Podgorica to assist Dikic's group in the planned post-election clashes. Linked through

their encrypted phones to indicted Montenegrin plotter Milan Knezevic, the specialists terminated their operation due to the later radio silence. Without further intelligence from BIA, Montenegrin authorities believe that the GRU unit fled Montenegro through neighboring borders.

Two Russian agents distinct from the group in Zlatibor escaped into Serbia. These GRU operatives had been coordinating coup-related efforts within Montenegro in the months leading up to the election. As word of the plot's discovery spread, the two successfully made their way to Belgrade to and were later extricated back to Russia. A day after, the Security Council Secretary and former FSB chief Nikolai Patrushev, made a short, unplanned trip to Belgrade. Significantly, to mention, BIA communications with Montenegrin counterparts discontinued after Patrushev's trip to Belgrade. The two were tried in absentia in Podgorica. Another unusual link between the alleged perpetrators and Russian highest level of politicians has been uncovered when the Serbian authorities arrested at Podgorica's request two Serbian citizens in Belgrade, on 13 January 2017. Following their previous activities, one of them proved to be in the close proximity of the Russia's Foreign Minister, Serghei Lavrov, during his visit in Serbia, in December 2016, including in tight secured places of the visit (Radio Free Europe, Radio Liberty 2017). Very soon after the initial arrest, on 8 February 2017, the Belgrade High Court rejected Montenegro's request to extradite the two, saying the request was baseless (Radio Free Europe, Radio Liberty 2017).

On 9 May 2019, after a 19-month trial, 13 people were sentenced over the 2016 failed coup for attempting an act of terrorism. Among them, in absentia, the two Russian GRU operatives (15, respectively 12 years in jail), two members of the FD to five year jail terms each, and Bratislav Dikic to eight years (Radio Free Europe, Radio Liberty 2017).

The Montenegrin Appeals Court on 5 February 2021 cancelled the initial decisions against the suspects, mentioning "significant violations of criminal procedure," and requested the High Court to retake the trial (Radio Free Europe, Radio Liberty 2021).

Moscow authorities has repeatedly dismissed at all levels the accusations about their role as being absurd.

CONCLUSIONS

Hostile military intelligence services execute operations on the territories of perceived enemy countries no matter the military strength of these or possible consequences. In perpetrating the aggressive operations, intelligence services use a vast array of asymmetric means, employing high-end technological tools and facilities.

Despite the effort to cover their actions, the technological developments also permit to professionals in the attacked countries to attribute most of the assaults and indict the wrongdoers. Unfortunately, due to the lack of legal means at the international level, most of the perpetrators remain unpunished. Worth mentioning is that even when the attacks are repeated on the same country (United Kingdom) and using the same tactics and procedures (poisoning political opponents), and the leadership is well aware of the deed amounting to an act of war and the responsible country (Bolton 2020), the retaliation measures are weak and non-efficient.

Global in nature, the hostile operations presented show that, through steady, trustworthy cooperation among allies, the intelligence services can uncover them and point to the evil organizations. On the same time, sharing the knowledge can help preventing or mitigating the effects of the aggressiveness. Romania's national security considered alone or in conjunction with those of its allies could be ensured only if the threats are known and countered with strength and professionalism.

Beyond providing awareness to the asymmetrical / hybrid threats, efforts on discouraging such acts are needed, and international legislation adapted to the current reality. Failure in punishing the unfriendly operations would only inspire wicked countries and private entities to act again with undesired consequences on people wellbeing.

Romania's security umbrella, constituted by the membership in NATO and EU, as well as the strategic partnership with United States is offering a wide array of tools, ranging from military to economic, political, social and judicial, to counter the conventional and unconventional threats.

However, the national effort is decisive and should raise to the reality of the present global challenges.

REFERENCES

Council of the European Union, "European Security Strategy", 8.12.2003, https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf. 3

Council of the European Union, "European Security Strategy", 8.12.2003, https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf. 8. "*In an era of globalization, distant threats may be as much a concern as those that are near at hand... The first line of defense will be often be abroad. The new threats are dynamic...Conflict prevention and threat prevention cannot start too early*".

AAP-06, "NATO Glossary of Terms and Definitions Edition 2019", promulgated by *NATO STANDARDIZATION OFFICE (NSO)* on 11 November 2019, Brussels. 15; 64.

Fiott, Daniel, Parkes, Roderick. 2019. "Protecting Europe, The EU's Response to Hybrid Threats", *European Union Institute for Security Studies, Chaillot Paper 151*, April, Published by Bietlot in Belgium. 45.

European Parliament, European Commission. 2016. "Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats. A European Union response", Brussels, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN. 2

European Center of Excellence for Countering Hybrid Threats. February 2021. https://www.hybridcoe.fi/hybrid-threats/,. Front page

Guide of the National Defense Strategy for 2015 – 2019, chapter Glossary for the Main Concepts of SNAP, http://old.presidency.ro/static/Ghid%20SNApT_2015-2019_AP.pdf. 8

Presidential Administration. 2020. "Strategia Națională de Apărare a Țării Pentru Perioada 2020-2024", Bucharest, DSN 1/794 din 26.05.2020.

Presidential Administration. 2020. "Strategia Națională de Apărare a Țării Pentru Perioada 2020-2024", Bucharest, DSN 1/794 din 26.05.2020, Paragraph 50. 12.

Ministry of National Defense. 2020. "White Book of Defense", Bucharest.

NATO. "NATO's response to hybrid threats". 08 August 2019. Accessed on February 2021. https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO. "Secretary General participates in Hybrid Centre of Excellence inauguration with Finnish leaders and EU High Representative", Accessed in February 2021. https://www.nato.int/cps/en/natohq/news_147497.htm, 2 October 2017

European Commission. 2020. "Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats", Brussels, 24 July 2020. 1

Council of the European Union. 2019. "Complementary efforts to enhance resilience and counter hybrid threats – Council Conclusions (10 December 2019)", Brussels, 10 December 2019.

European External Action Service. 2019. EU Military Staff, *Impetus Magazine*, "Single Intelligence Analysis Capacity (SIAC) and its role in supporting EU decision making" Autumn/Winter 2019, Number 28. 10.

Department of Justice. 2018. Office of Public Affairs, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations", 4 Oct 2018. 1

Ministry of Defense (Ministerie van Defensie). 2018. Militaire Inlichtingen- en Veiligheidsdienst, Genmaj. O. Eichelsheim, “GRU close access-cyberoperatie tegen OPCW”, 4 Oct 2018. 1-35.

Reuters, Vasiljevic, Stevo. 09 May 2019. “Russians, opposition figures sentenced over role in 2016 Montenegro coup attempt”. Accessed February 2021. https://www.reuters.com/article/us-montenegro-court-idUSKCN1SF144

Foreign Policy Research Institute, Reuf, Bajrović, Vesko, Garčević & Richard, Kraemer. June 2018. “Hanging by a Thread: Russia’s Strategy of Destabilization in Montenegro”. Accessed February 2021. https://www.fpri.org/wp-content/uploads/2018/07/kraemer-rfp5.pdf

Radio Free Europe, Radio Liberty. 13 January 2017. “Serbia: Two Suspects Detained In Alleged Montenegro Coup Attempt”. Accessed February 2021. https://www.rferl.org/a/serbia-arrests-montenegro-coup-suspects-ristic-bogicevic/28231807.html

Radio Free Europe, Radio Liberty. 10 February 2017. “Serbian Court Rejects Montenegrin Request to Extradite Suspect in Alleged Coup Attempt”. Accessed February 2021. https://www.rferl.org/a/serbia-court-rejects-montenegro-request-extradition-alleged-coup-plot/28301782.html

Reuters, Vasiljevic, Stevo. 09 May 2019. “Russians, opposition figures sentenced over role in 2016 Montenegro coup attempt”. Accessed February 2021. https://www.reuters.com/article/us-montenegro-court-idUSKCN1SF144

Radio Free Europe. Radio Liberty. 5 February 2021. “Montenegro Court Overturns 'Coup Plot' Verdicts”. Accessed 27 February 2021. https://www.rferl.org/a/montenegro-court-overturns-coup-plot-verdicts/31088156.html

Bolton, Michael, The Room. 2018. During the meeting in London on 13 July among Donald Trump, John Bolton, Theresa May, Jeremy Hunt and Mark Sedvill (Cabinet Secretary and Head of the Home Civil Service – UK), the later referred to the poisoning operation of Serghei Skripal “as a chemical weapons attack on a nuclear power.” 137