Cybersecurity and Hybrid Warfare Challenges in the Black Sea Region

Silviu NATE, Leonela LECA
Global Studies Center, Lucian Blaga University of Sibiu
silviu.nate@ulbsibiu.ro, leonela.leca@gmail.com

Abstract: The Black Sea region is the new frontline of the hybrid warfare. It is dominated by the discrepancies between the technological penetration, the insufficiently integrated tools and means to counter the cyber warfare and the unprecedented level of the combined conventional and nonconventional threats to the regional and EU security environment. The aim of the present paper is to highlight the need to enhance the level of regional cooperation in countering hybrid threats that are a part of the hybrid warfare against Ukraine.
Keywords: Black Sea militarisation, Energy security, Hybrid warfare, Asymmetric warfare cyber warfare, Cyber security.

INTRODUCTION

While war has always been a complex set of interconnected threats and means in order to pursue political goals, "hybrid" still remains an elusive and captivating term. The evolution of modern conflict is influenced by technological dynamics and tactics change according to available resources, which are able to influence the social, political, economic or military outcome. Therefore, "every age has its own kind of war, its own limiting conditions, and its own peculiar preconceptions" (Howard and Paret on Clausewitz, 1989). Hybrid warfare refers to irregular and disproportionate methods to counteract a higher conventional force (Fleming, 2011).

Actors using hybrid measures can engage in a proxy war – a conflict between two states or non-state actors, in which neither entity directly engages the other, but has independent and undeclared agendas.

They use a unified strategy, mixed tactics and an arsenal that includes: conventional capabilities, irregular tactics, diplomacy, politics, terrorist acts, cyber-attacks, non-discriminatory violence, and criminal activity. At the same time, hybrid warfare is a marriage between technology and conventional methods that develops as a fighting tool for the next generation (Asian Warrior, 2016).

Consequently, we assert that a hybrid adversary uses clandestine and disproportionate actions to avoid attributing his actions and taking responsibility. Those tactics make it difficult to legitimize a traditional defensive response from the defending party.

Preventing, assessing and responding to the progressively evolving and complex security challenges requires multi-domain action. Although it started with the 2008 Russian invasion of Georgia, it was not until the 2014 military action in Ukraine and the illegal annexation of Crimea that European Union and NATO countries, even though not always synchronized, sought to renew and update solutions in order to counteract the new, more complex type of challenges.

The conventional conflict's means and tools have steadily become obsolete in recent years, in favor of non-kinetic means and other tools. The Russian military intervention in Ukraine, the seizing of Crimea, the continuing military buildup and taking control over a major part of the Black Sea through both conventional and non-kinetic means represents a hallmark in the hybrid warfare model. Russia applies hybrid warfare strategies not only to create a greater impact with minimum expenditure and losses in achieving strategic goals of foreign policy but also to abuse or avoid the normative dispositions of the international law and treaties while staying just below the threshold of Article 5. Other examples of lawfare include using The Montreux Convention Regarding the Regime of the Straits (Harry, 1936) or the Danube Commission (Danube Commission, 2020) in its own interests.

The intensity of the use of Russia's hybrid methods against Ukraine has increased international interest and awakened NATO's desire to understand the peculiarities of this form of aggressive action. As a result, and dependent on their goals, the Alliance has focused on the study of methods of combining covert and overt military presence, information warfare, cyber warfare, and economic warfare (Yevhen, 2018).

Hybrid threats include various coercive activities that jeopardize security by conventional or unconventional means and the methods are diplomatic, military, economic or technological. Cyber-attacks, election interference, disinformation campaigns, the undermining of economic activity or the disruption of critical infrastructure facilities, transport and communication routes are only a few examples of hybrid tools.

As stated above, hybrid warfare is a complex type of conflict, a way to fight without fighting openly, the definition of hybrid warfare is therefore flexible in order to respond to the scalable nature of these type threats.

According to NATO's definition, hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and the use of regular forces. Hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations (NATO, 2019).

In the European Union's view, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalize, recruit and direct proxy actors can be vehicles for hybrid threats (European Parliament, 2016).

The online environment represents an ecosystem of individual, political and financial actors and actions, but also an area of intellectual fusions. When referring to cybercrime, non-state actors and criminal groups might exploit cyber-space for a variety of fairly predictable purposes, including money laundering, drug trafficking, extortion, credit card and ATM fraud, software piracy, industrial espionage, counterfeit documentation and so on (Choo and Smith, 2008).

Cyber became an integral warfare domain joining those of the traditional land, air, sea, and space. Cyber-attacks are currently listed among the top offensive tools of a potential adversary

along with such classic instruments as submarines or special operations (SpecOps) teams. The recent discussion of the Islamic Republic of Iran to retaliate digitally for the deadly US attack on the high ranking General Soleimani concludes that kinetic and cyber offense currently exists within the same framework and one could be a substitute for another (Kremez, 2020).

Cyber warfare allows greater flexibility for carrying out attacks across great distances and against more powerful adversaries, all while denying involvement in the conflict. Cyber operations mean conflicts can be carried out at a global level with relatively modest resources, erasing geographical boundaries, with significant spillover effects from one target to a larger impact (Danyk, Briggs, and Maliarchuk, 2020).

Meanwhile, adversaries may use (cyber-) terrorism to create fear in an attempt to coerce or intimidate governments or societies and to gain control over the population (NATO, 2018).

The hybrid war that incorporates cyber-attacks usually aims to carry out "kinetic attacks", to support traditional war tactics. The only difference from the traditional model is that the attacks can be remotely orchestrated and the insidious cyber weapon can be a false flag.

For example, the activity of the alleged "Cyber Caliphate" affiliated with ISIS, which targeted databases of the US military, was in fact a false flag operation, carried out by the Russian hacking-sponsored group APT 28.

The infiltration of critical infrastructures by external entities, data and industrial espionage for gathering advanced knowledge and the search for illicit economic gains justify the need to refine cyber capability.

We conclude that cyberwarfare represents the use of technology to attack a nation, causing significant injury to actual hardware, infrastructure, data and to manipulate human beliefs. Undoubtedly, it may be a substantial component of hybrid warfare.

THEORETICAL BOUNDARIES

From a realist's perspective, mixing hard and soft-power components in hybrid warfare creates operational and retaliation difficulties by traditional means. When it comes to hybrid warfare and cyber-attacks, weapons of mass destruction are no longer the fundamental substitute for achieving a balance of power. Therefore, the new international system tends to move towards multipolarity and greater volatility of the security environment.

The liberal paradigm is strongly undermined by the hybrid nature of threats. Its clandestine character and the inability to legitimize an offensive act, leads to the impossibility of identifying an aggressor and applying international norms. Amid relationships characterized by ambiguity, cooperation and peace-making efforts are almost impossible. In this case, technological interdependencies rather create a viral phenomenon and a contagion.

Societal security is mainly affected by manipulative actions and influence operations. Active measures, informational warfare and cyber-attacks aim to demoralize and weaken communities' resilience to aggressors. Consequently, technology plays an important role in a conflict, but understanding the awareness, intention and tactics behind these tools are crucial.

RESEARCH QUESTIONS

Through this paper we try to answer the following questions:

1. What are the trends/variables that influence the security environment in the Black Sea region?
2. What solutions and mechanisms can be identified to prevent cyber and hybrid aggression in the Black Sea region?
3. How can the mechanism of regional cooperation be enhanced to increase cyber resilience?

MAPPING SECURITY CHALLENGES FOR THE BLACK SEA REGION

The lack of a consensus of allies on the Black Sea region, without an objective assessment of the need for strategic defense in the Black Sea, and the absence of a major regional project to design security and stability in the Black Sea, led to disproportionate involvement of allies and littoral actors. Eastern Partnership countries have limited integrated attitudes; they are often fragmented by geopolitical negotiations between the EU and Russia.

Following the 2018 Brussels Summit, there are clear signs that the NATO Strategy for the Black Sea has evolved and became more focused. Reflection circles, foreign and Romanian, have become more committed to this issue, providing operational and political recommendations for the two key institutions, NATO and the EU, to tackle more effectively the security issue in the Black Sea Region.

The added value of the security policy lies in the direct involvement of the US and the expansion of multinational exercises, raising awareness of the main regional challenges and risks, and developing active measures to balance and combat not only conventional but also unconventional threats such as terrorism, organized crime, illegal migration, etc.

The regional situation indicates that the countries of the Black Sea Region are no longer focusing on security as an integrated regional phenomenon, but are currently focusing on managing their own domestic problems and needs, developing competing security agendas or, at most, bilateral relations.

Over the last decade, Russia has jumped from partner to competitor and even adversary, showing aggressive behavior by violating international law and using force. Russia's behavior tends to be projected in the long run and will continue to test the response capacity of NATO and its partners. Also, one can see a unitary perception of how the Black Sea littoral states perceive Russia.

The Black Sea region is at the point of overlapping interests of several regional and extra-regional actors; it has become a new strategic border for Europe, Russia and the United States in terms of energy security and is an intersection of different values and cultures: European, and Asian.

The nature of security threats in the region range from conventional to unconventional or hybrid methods; In addition, the regional climate includes the existence of frozen conflicts and "hot spots" (Transdniestria, Abkhazia and South Ossetia, Donetsk and Luhansk), poorly

secured transport routes, illegal migration, corruption, organized crime, terrorism, and attacks exploiting cyber vulnerabilities.

Crimea is being militarized strategically in the long term, but, right now, it is done in the context of the conflict in Syria. This way, Russia tends to incorporate the Black Sea into a larger conflict zone, making weapon supply routes possible from Crimea through the Bosporus and Dardanelles Straits, then through the Mediterranean Sea to the military bases in Syria, and later to Libya.

In the Black Sea region, Ukraine became the front line for hybrid and cyber-attacks and could represent the pilot project for future hybrid operations. Open warfare with Russia and the Kremlin's seized control over Crimea, Azov Sea and the major communication and energy assets along with the vulnerable political and economic environment, have made the country the perfect laboratory for those looking to test new cyberweapons, tactics, and tools.

Russia is a significant cyber power with advanced technological and human capabilities. It has integrated cyber tools in promoting its foreign and security policy at a higher level than other states (Znak.com, 2019). Moreover, Russia is using cyber operations as a coercive tool in addition to the disinformation campaigns.

If, in 2007, Russian cyber-attacks began first as denial of service attacks against a considerable part of the Estonian economy and government and continued in the Russian conflict with Georgia in 2008, the scale of cyberespionage in Ukraine has become unprecedented.

The evidence of Russian connected malware goes back to 2010. Analyses of cyber-attacks on Ukraine demonstrate the main destabilizing goals of these attacks and that the incidents were not isolated. Destabilizing vital systems of the country, governmental institutions' activity, as well as critical infrastructures and the use of social media to target specific individuals are part of these goals.

The situation changed dramatically after 2014. In December 2015, Ukraine suffered the first significant cyberattack on its electric grid. The attack affected approximately 250,000 customers for some hours, but appeared to have no lasting damage despite targeting the Supervisory Control and Data Acquisition (SCADA) controllers that control mechanical processes in addition to business-system workstations and servers. The malware employed in the cyberattack was a set of tools, including the BlackEnergy Trojan and the KillDisk eraser, that targeted at least three geographically diverse regional power substations. The impact on the energy sector received the most attention, as the attack occurred during Ukraine's cold winter season, but the cyber operations against Ukraine also impacted the media, finance, and transportation sectors. The Ukrainian government ties these activities to Russian security services. Attacks on various sectors continued in 2016, including another attack that hit the Kyiv transmission station almost exactly a year after the December 2015 attacks (Hodgson, Ma, Marcinek, and Schwindt, 2019).

In 2017, a cybersecurity company, Palo Alto Networks, discovered another Russian cyber espionage operation in Ukrainian networks – the Gamaredon Group that had been active at least since 2013. Another cybersecurity company discovered the Russian cyber espionage campaign, Operation Armageddon, which, according to them, had targeted officials in the Ukrainian military and national security establishment in 2013-2015. The Ukrainian security services attributed the cyberespionage to their Russian counterparts (Pernik, 2018).

The June 2017 attack, delivered through a mock ransomware virus dubbed NotPetya, wiped data from the computers of banks, energy firms, senior government officials and an airport. The GRU military spy agency created NotPetya, the CIA concluded with "high confidence" in November, according to classified reports cited by U.S. intelligence officials (Nakashima, 2018). Later, in October 2017, ransomware named BadRabbit encrypted hard drives and rendered IT inoperable. This caused disruption including to the Kyiv metro, Odessa airport, Russia's central bank and 2 Russian media outlets.

The governments of Britain and the US declared that Russia's military intelligence service GRU was behind the massive cyber-attack that hit Georgia during 2019. In October 2019, a wave of cyber-attacks hit 2,000 websites in Georgia, including the sites of the president, courts, and local media (Paganini, 2018). At the same time, Romania recorded 63.32% cyber-attacks from China and 5.85% from Russia (CERT-RO, 2018).

The critical infrastructures in NATO and EU Member States is a potential target for hybrid threats, including through cyber interference. Moreover, energy infrastructure is extremely vulnerable, and disruptions may cause brownouts or even blackouts which have a major national and regional economic impact. Throughout recent history, Russia has used this type of disruption (the 2006, 2009 gas crisis, the cyber-attacks on the electricity grids or SCADA systems in Ukraine) in order to affect the country's capacity and credibility to ensure a stable transit of energy towards the European Union. If analyzing the broader context of the perspectives of the energy market integration of Ukraine and a future single digital market, strengthening the cyber defence capabilities of the Eastern flank of NATO and the EU becomes vital for the wider region not only in terms of security but also in terms of economic sustainability. The integration of power systems and gas networks of Ukraine and the Republic of Moldova with the grid of continental Europe and the digitalization of energy markets and distributed networks must be synchronized with measures that enhance the cyber security.

At the present moment, tensions following the situation in the Azov Sea and Russian control of the Kerch Strait through the 6 FSB Coast Guards Units pose significant risks associated with the transportation system and cargo inspections.

Beside this control over Azov sea, after the illegal annexation of Crimea, Russia took over the 4 drilling platforms – Tavrida, Syvash, Petro Hodovanets and Ukrayna. The Russian organization Cernomornaftogaz lobbied the government to declare these platforms as critical infrastructures and installed radars and military (including cyber) capabilities at those sites. Moreover, military exercises, the so-called snap exercises are organized near the international shipping routes forcing the latter to be re-routed. The purpose is twofold: to project strength and to enhance command and control capabilities. Thus, the Northern part of the Black Sea towards Odessa is also hampered by Russian actions that are increasing the economic, investment, insurance and the overall transportation risk. Referring to Ukraine's potential role in the transportation corridor connecting China to Europe (Ukraine being one of the first countries that signed three agreements for the Belt and Road Initiative, the whole transportation corridor is hampered by Russian military build-up and anti-access and area denial measures.

A recent dynamic is extremely important for the EU's economic zone within the Black Sea. Last year, the US energy giant, Exxon Mobil, announced its intention to exit the Romanian Neptun Deep offshore project located in the Black Sea. It is an extremely important project for Romania and for

the region. Exxon owns 50% of the Neptun Deep, the rest is owned by OMV Petrom. The Russian company Lukoil announced its interest in buying Exxon's shares. The proximity of the naval zones controlled by Russia to the Romanian Exclusive Economic Zone increases the investment risk, with the Neptun Deep Shore project already becoming a key economic and security project.

The challenges that the Black Sea region is facing needs to be addressed in a systemic, coherent and coordinated way. There is a need to review and to strengthen the mechanisms of coordination/cooperation between NATO and Ukraine and/or European Union and Ukraine. The existing NATO Comprehensive Assistance Package for Ukraine, NATO's Exercises in the Black Sea Area as well as the Joint Working Groups on Defence Reform and on Defence Technical Cooperation, need to have the interoperability dimension in order to ensure permanently interoperable structures. Relative steps were taken in reviewing the NATO's Comprehensive Assistance Package for Ukraine by offering support to Ukraine, in areas such as command and control and cyber defence.

In the cyber field, the NATO-Ukraine Trust Fund on Cyber Defence was signed on 2 December 2014, Romania being designated as the lead-nation.

Nevertheless, in order to deliver real results, strengthening regional resilience to hybrid threats and cyber-attacks must be addressed in a more coherent and operationalized manner.

POLICY DEBATES AND ACTIONS

The European Union and NATO face dynamic cyber challenges. The exchange of good practices, the exchange of information and the organization of bilateral meetings contribute to a better strategic understanding and the identification of appropriate mechanisms (NATO Communications Team, 2019).

NATO-EU cooperation focuses on cyber concepts and doctrines, training and education courses, threat indicators, ad-hoc exchanges of alerts and assessments on threats, interinstitutional information, including cyber aspects of crisis management and periodic meetings (European Union, 2019).

In the EU, 87% respondents see cybercrime as important and this is the case for a majority of respondents in every country. This proportion has increased by seven percentage points since March 2015 (European Commission, 2017).

From NATO's perspective, areas where technology could revolutionize warfare are subsurface and subterranean operations, swarm techniques, space-based weapons, directed energy, autonomous systems and sensors, quantum computing, unmanned systems, electromagnetically launched projectiles, renewable energy, artificial intelligence, additive manufacturing/3D printing, biotechnology, and nanotechnology.

By understanding the need to integrate a joint comprehensive plan for the Baltics and the Black Sea in the non-military realm, cyber security cooperation can be increased in the region and joint training programs initiated. Several initiatives can be undertaken in the energy sphere, including developing regional infrastructure such as an LNG corridor and synchronizing the region's electricity system (Hodges, Bugajski and Doran, 2019).

RECOMMENDATIONS

The following recommendation require sustained diplomatic efforts on behalf od trained diplomats, experts and decision makers to implement.

Firstly, the creation of permanent mechanisms of Security and Defence integration. In reviewing the tools to address the complex security challenges that the Black Sea is facing, the permanent mechanisms of Security and Defence integration must be created and implemented. In order to create permanent structures that would be capable to respond to cyber threats, the establishment of operational and integrated centers for rapid response to cyber threats is necessary and can be based on the model of NATO Cooperative Cyber Centre for Excellence from Estonia. Another goal is to update the cyber defense commitment - setting a threshold that could determine the extent to which a cyber-attack can be considered for triggering NATO's Article 5.

Secondly, we must identify solutions at NATO level to ensure free movement in the Black Sea. There is a need to ensure the security of the maritime energy infrastructure and transport corridors in the Black Sea. Common efforts to ensure the free movement must be organized and funded. Communications and cyber security components must be protected.

Stakeholders must also pursue the enhancement of regional cooperation and the creation of multi-annual programs. Estonia's example could serve them well, since the country has fostered an intense focus on the internet and cyber threats. Nevertheless, the regional dynamic of the malicious actors who also pose significant threats to the other Baltic states' cyber and communications infrastructures, led all three Baltic countries to sign a memorandum of understanding in November 2015 to promote cooperation in this area. Potential measures include: enhancing bilateral, trilateral and regional cooperation and integration through the establishment of operational and integrated centers for rapid response to cyber threats; common multi-annual programs, various scenario-based tests for cybersecurity incident response capabilities, the creation of permanent task-forces that would include governmental and private entities using the ENISA model to create a platform for exchange of best practices. Moreover, common approaches to standardization and protection methodologies are needed in order to strengthen resilience to hybrid threats and cyber-attacks. Other measures include repeated exercises simulating a cyber-attack accompanied by the simulation of a hostile campaign of strategic communication leading into early warning and joint efforts to achieve the objectives of countering cyber-attacks and managing critical infrastructure protection.

Lastly, we must define, identify, designate and defend critical infrastructure. Regional networks and infrastructure represent a potential target for hybrid interference and cyber-attacks. Both physical security and cyber security must be addressed. It is worth noting that Romania needs to develop a strategy for digitalization in energy. Regional energy interconnection projects must also include the digitalization strategies/options and (cyber) security mechanisms.

REFERENCE LIST

Asian Warrior. (2016). Hybrid Warfare: The Next Generation Tool, available at https://www.asianwarrior.com/2016/09/hybrid-warfare-the-next-generation-tool-unitedstates-russia-china-pakistan.html

CERT-RO. (2019). Evoluția amenințărilor în spațiul cibernetic românesc în anul 2018, p.7, available at https://cert.ro/vezi/document/raport-alerte-2018

Choo, K.R. and R. G. Smith. (2008). Criminal Exploitation of Online Systems by Organised Crime Groups, Asian Criminology, Vol. 3, No. 1, June 2008, p.40.

Commission, E. (2017). Europeans attitudes towards cyber security. Special Eurobarometer 464a, available at: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171

Danyk, Y. Briggs, C. and Maliarchuk T. (2020). Hitting Home: Cyber-Hybrid Warfare in Ukraine and Its Impact on the United States, Georgetown Journal of International Affairs, available at https://gjia.georgetown.edu/2020/02/18/cyber-hybrid-warfare-in-ukraine-and-impact-on-united-states/

European Parliament. (2018). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final, available at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52016JC0018

European Union. (2019). EU-NATO Cooperation, available at https://eeas.europa.eu/sites/eeas/files/eu-nato_cooperation_factsheet_june_2019.pdf

Fleming, Brian P. (2011). Hybrid threat concept: contemporary war, military planning and the advent of unrestricted operational art, United States Army Command and General Staff College, p. 15.

Hodges, Ben, Bugajski, Janusz and Doran, Peter B. (2019). Strengthening NATO's Eastern Flank – A Strategy for Baltic-Black Sea Coherence, Center for European Policy Analysis, available at https://1f3d3593-8810-425c-bc7f-8988c808b72b.filesusr.com/ugd/644196_8754c3428d9d4da0adb29bef6df2f5b4.pdf

Hodgson, Quentin E., Ma Logan, Marcinek, Krystyna, and Schwindt, Karen. (2019). Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace. Santa Monica, CA: RAND Corporation, available at https://www.rand.org/pubs/research_reports/RR2961.html.

Howard, Harry N. (1936). The Straits After the Montreux Conference, Foreign Affairs, available at https://www.foreignaffairs.com/articles/turkey/1936-10-01/straits-after-montreux-conference

Howard, Michael, Paret, Peter (eds.) (1989). On War. Princeton, NJ: Princeton University Press. p. 593.

Kremez, Vitali. (2020). Pro-Russian CyberSpy Gamaredon Intensifies Ukrainian Security Targeting, Sentinel Labs, available at https://labs.sentinelone.com/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/

Nakashima, Ellen. (2018). Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes, The Washington Post, available at https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

NATO Communications Team. (2019). NATO and EU discuss cyber threats ahead of European elections, available at https://www.ncia.nato.int/NewsRoom/Pages/20190503-test.aspx

NATO. (2018). FRAMEWORK FOR FUTURE ALLIANCE OPERATIONS, available at https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf

NATO (2019). NATO's response to hybrid threats, available at https://www.nato.int/cps/en/natohq/topics_156338.htm.

Paganini, Pierluigi. (2018). UK, US and its allies blame Russia's GRU for 2019 cyber-attacks on Georgia, Security Affairs, available at https://securityaffairs.co/wordpress/98192/cyber-warfare-2/uk-us-blame-russia-gru-georgia.html

Pernik, Piret. (2018). The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine, Institute for Security Studies, Chaillot Papers, p. 61, available at https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

Danube Commission (2020), available at https://www.danubecommission.org/dc/en/danube-commission/

Yevhen, Mahda. (2018). Russia's hybrid aggression: Lessons for the world, Institute of World Policy, p. 37.

Znak.com (2019). Путин создал в МИД департамент по международной информационной безопасности, available at https://www.znak.com/2019-12-29/putin_sozdal_v_mid_departament_po_mezhdunarodnoy_informacionnoy_bezopasnosti

Silviu NATE
Assoc. Prof., Ph.D. holds the director's position at the Global Studies Center, Lucian Blaga University of Sibiu. Dr. Nate has a background in Political Science and Security Studies, he conducted several research projects related to EU Energy Strategy, migration, transatlantic and Black Sea strategic issues; he is a member of the Euro-Atlantic Council Romania.

Leonela LECA
PhD (c), Global Studies Center, Lucian Blaga University of Sibiu, Romania, Romania, Researcher, expert on energy security with the focus on the energy diplomacy, Caspian Sea and Black Sea region. For over 12 years she held the position of Vice-President, co-founder, member of the Board and Head of Economic and Energy Department in several national and international Think Tanks. Also, for five years she acted as international market advisor, being involved in strategic business development promoting complex integrated IT Security projects in the Black Sea and Caspian Sea Region.