RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

THE EUROPEAN PERSPECTIVE OF THE ANTI-WESTERN INFORMATION WARFARE

EREKLE IANTBELIDZE

EXPERT OPINION 165

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

EXPERT OPINION

EREKLE IANTBELIDZE

THE EUROPEAN PERSPECTIVE OF THE ANTI-WESTERN INFORMATION WARFARE

165

2021

The publication is made possible with the support of the US Embassy in Georgia. The views expressed in the publication are the sole responsibility of the author and do not in any way represent the views of the Embassy.

Technical Editor: Artem Melik-Nubarov

ISSN 1512-4835
ISBN

"Although our eyes cannot penetrate the darkness of the future, scientific geopolitical analysis enables us to make certain predictions." – Karl Haushofer, 1942.

(Gearóid Ó Tuathail, 2003).

Introduction

The transfer of the international political reality to a new multi-polar prism makes geopolitics, as one of the directions of interdisciplinary education, more important in the current situation. The development of digital and scientific technologies has moved the phenomenon of the balance of power to a new stage and for a number of states and intergovernmental organizations, the term geopolitics has become the flagship of security strategy, cultural domination and democratic processes. In terms of the new "geopolitical commission," the action plan of Ursula von der Leyen rests on two main principles – Europe's climate and digital transition (European Parliament, 2020). Therefore, in the conditions of a war of values, geopolitics and digitalization, technological development has become a super-important component that the European Union is attempting to bring to the forefront as it wrestles with the world's foremost states (China, India, Russia, Turkey). As the EU's top diplomat, Josep Borrell, stated, Europe must not become a playground for other great powers and it must take the role of a geopolitical leader in the world (Barigazzi, 2019). It must also be pointed out that the geopolitical nature of Europe also envisages the development and gradual expansion of its neighborhood policy. That said, the associated partners within the Eastern Partnership (EaP) format (Moldova, Georgia, Ukraine) have bigger ambitions and goals than the development of the Deep and Comprehensive Free Trade Area (DCFTA) and the full implementation of the Association Agreement (AA) (European Commission, 2019).

From a regional standpoint, the occupation of Georgia's territories by Russia in August 2008 as well as the annexation of Crimea in 2014 and launching armed conflict in the Donbas region became the main sources for unmasking Russian hybrid warfare. As a result, this aforementioned form of warfare became a cause for alarm for multiple European states as well as being one of the main reasons for domestic political polarization. While Sweden and Poland openly support close cooperation with the Eastern Partners in terms of security, other member states of the EU reject

developing political processes in this direction, including differentiation and inclusivity in terms of the neighborhood policy format (Gerasimov, 2020). Despite this, apart from the associated partners, Azerbaijan also expresses its desire to cooperate with the European Union in terms of overcoming hybrid warfare, disinformation and propaganda and developing soft security.

The abovementioned political developments and the conflict of interests make it necessary for the member states of the European Union to take unified and concrete European steps, creating functional mechanisms (apart from the EU Security Union Strategy 2020-2024) for overcoming hybrid warfare. Therefore, the goal of this paper is to:

- Analyze the European Union's role in opposing anti-Western hybrid warfare;
- Assess the importance of Russian propaganda and disinformation in the domestic political processes of the European states;
- Explain the importance of the Eastern Partnership in overcoming disinformation and bolstering European security.

The European Union and the Russian "Maskirovka (2.0)"

It is no longer a surprise for any European state or the European Union at large that the Russian Federation often utilizes old Soviet practices. Hence, the Soviet past has also not been discarded in terms of security and hybrid warfare. The so-called doctrine of "Maskirovka," that combined tactical calculations and principles, was often used by the Red Army in military action (Elliott, 2018). Nowadays, Russia has further developed this concept both theoretically and practically, adding a host of governmental capacities as well, which include media manipulation, trade in energy resources and fuel, political agitation, cyber-attacks, encouraging the so-called surrogate military powers, implanting agents and provoking anti-state processes (Roberts, 2015). It is also important to note that given its constant adaptation, this doctrine attempts to identify those weak points of a given state that would allow it to instantly react to political destabilization, polarization of public opinion and radicalization (Vowell, 2015).

Russia's military, political, administrative and media outlets are, it would be fair to say, masters of practicing "Maskirovka (2.0)." In response to this, the European Union does not have a unified or holistic approach that could

serve to contain Russian anti-Western information warfare. On the other hand, the Cyber Diplomacy Toolbox created by the European Union Agency for Cybersecurity (ENISA) in 2017 and the functioning of the European Cybersecurity Competence Centre and Network must also be pointed out (Pawlak, 2017). With the use of these capacities, security measures are observed on an internal institutional level, avoiding potential cyber-attacks. In terms of more large-scale endeavors, the European Union has thus far been spending quite a small amount of financial or technological resources which further emboldens Russian special forces to project their power in Western states. As Vladimir Putin's special representative in information security affairs points out, Russia is a cyber-giant while the European Union is a small and irrelevant barking dog (Gressel, 2019).

The mistake of the states and institutions united under common European values was that it took too long for the allied states to understand what M. Weiss and P. Pomerantsev call the "weaponization of culture and ideas" under Russia's anti-Western policy (Weiss, 2014). Therefore, in 2015 the Council of the European Union took the first step and a digital platform was created under the European External Action Service (EEAS) entitled the East StratCom Task Force through which, at the first stage, up to 4,000 propagandist and disinformation stories were revealed and publicized (www.euvsdisinfo.eu) on the website. Additionally, according to the 2016 resolution of the European Parliament, the aforementioned institution got the very first budgetary funding of EUR 1.1 million with the priority being the unmasking of Russia's anti-Western propaganda through social media platforms (Twitter, Facebook, Instagram) (European Parliament, 2019). These concrete steps taken by the European Union had positive results in terms of revealing fake news; however, individual member states and European institutions have much more work to do in terms of developing digital platforms, coordinating strategies and raising the awareness of citizens.

Fortunately, in terms of its Permanent Structured Cooperation (PESCO), the European security and defense policy envisages the implementation of important projects in the directions of cyber-security and counter-intelligence. Among them, the rapid reaction and mutual support program in the case of a cyber-attack is worth noting. The improvement of the strategic management and control (C2) systems in terms of reacting to cyber threats and incidents is also notable (EU Cyber Direct, 2019). Despite this, due to its structure and goals, PESCO is one of the main bases for

the interest of conflicts among the member states of the European Union. Part of the politicians see this cooperation format as a future guarantee of European security while another part of technocrats rejects the creation of some sort of a military alliance within the Union. Hence, given insufficient coordination and a conflict of interests, the European Union and its subsidiary institutions are hard-pressed to deal with the anti-Western intentions of the Russian "Maskirovka (2.0)."

European Elections and the "Illusion of Truth"

> *"If a lie is only printed often enough, it becomes a quasi-truth, and if such a truth is repeated often enough, it becomes an article of belief, a dogma and men will die for it." – Isabelle Blagden, 1869*.
>
> (Stafford, 2016).

The rethinking of Russian hybrid warfare is, of course, also taking place on an intra-state level throughout Europe. The societies of Western states are often victims of Russian disinformation manipulation. Claiming falsehoods and anti-Western rhetoric is usually done on a daily basis. Despite this, the government of Russia typically mobilizes resources ahead of elections when influencing public opinion is quite easy and emotions run high. Russian "soft power" mechanisms operate in almost all European states. Among them, the news outlets are notable, namely Sputnik News and Russia Today. Russia supports all methods that destabilize European politics which became clear during the referendums in Scotland and Catalonia. Another example was the "yellow vest" protests in France (Gressel, 2019).

In response to Russian hybrid warfare, some European states designated special units, as well as diplomatic representatives, which coordinate the unmasking of disinformation threats. Such countries include Lithuania, Finland, Poland, Sweden and Spain. As for Germany and France, both are trying to unmask Russian anti-Western actions indirectly without it taking on a political character. In the cases of Hungary, Austria and Italy, the governments do not consider the threats posed by disinformation warfare to be a priority and refrain from confronting Russia in terms of defense and security issues. It is not surprising that the Western world was shocked by the usage of Russian "bots," "trolls" and "accounts" during the Brexit referendum. As the F-Secure organization states, Twitter and Facebook accounts were used to spread disinformation and propaganda narratives (Ellyatt, 2020). European values were satirized and the European Union

was stigmatized on a digital level. The financial expenditure of the Russian Federation during the British referendum is worthy of attention. A study by the Hanns Seidel Foundation shows that Russia spent a total of GBP 1,353,000 of which GBP 102,000 was used for Facebook accounts while an amount ranging from GBP 50,000 to GBP 100,000 was spent on Twitter accounts (Špalková, 2018). In addition, the media outlets controlled by the Kremlin managed to negatively influence about 134 million voters, including 11 million Brits living abroad.

One of the most notable examples of overcoming Russian disinformation efforts was observed in France in 2017. Because of a cyber and information attack during Emmanuel Macron's presidential campaign, images, invoices and personal documents containing fake materials about the presidential candidate were disseminated. As the Head of the Center for Strategic and International Studies, Heather A. Conley, states, French political institutions were prepared for the cyber-attacks and managed to reveal fake materials quickly. The French political centralization practice (as surprising as that may be!) also played a major role. Through integrated and observational methods, the French intelligence services managed to reveal the source of the intervention; therefore, avoiding strong influence on the results of the presidential election (Bulckaert, 2018). Despite this, Russia's anti-Western information practice experienced a transformation and since 2018, Russia Today started gaining a foothold in the French information environment, supplying anti-Western political narratives to its audiences not only through TV broadcasting but also by using websites and social media.

Considering the abovementioned examples, we can say that Russia's disinformation strategy is very flexible and changeable. Despite the fact that the citizens of the European Union have high levels of political culture, overcoming the disinformation barriers is quite difficult and requires great mental and psychological resilience. Nowadays, no state, let alone an individual, is safe from being shrouded in the illusion of truth.

Eastern Partnership and "Mission Impossible"

Considering the European perspective, we can say that the Eastern Partnership region is the most fragile territory in terms of the dissemination of hybrid threats. As Rand Europe's study shows, the spheres of influence of Russian social media are the largest in this region which is due to a number of cultural, linguistic, religious and social-economic factors (Todd

C. Helmus, 2018). The role of anti-Western and disinformation propaganda flowing from Russia influence both the domestic as well as the foreign policy processes of states. The states such as Moldova, Georgia and Ukraine are united by their painful historical experience of relations with the Russian Federation. In addition, each of these states is occupied by Russian and separatist forces (despite the fact that in the case of Transnistria, Russia is taking the role of a potential "reconciler"). Religious and ethnic barriers create fertile ground for the Russian media outlets to influence large parts of the population and foment the polarization of public opinion. It is also important to note that the associated partners of the European Union are on the path of democratic transition with the trust of citizens towards state institutions being very low. Taking these and other elements into account, the Eastern Partnership region is a sort of a laboratory for modernizing and successfully transforming Russian hybrid strategies.

Every year, the media and state institutions inform us about Russian cyber-attacks and informational interventions in the elections processes of various states. In the Georgian reality, such an attack took place on October 15-17, 2019 on both private as well as public sector websites which did not specifically manage to unmask direct Russian or indeed any foreign intervention in Georgia's internet space; however, it gave the Western states even more cause to think about the necessity and importance of developing cyber security (Kakha Gogolashvili, 2019). Apart from this, another cyber-attack took place on September 1, 2020 on the Lugar Laboratory which was assessed to be a very serious threat given the COVID-19 pandemic (U.S. Embassy in Georgia, 2020). A disinformation campaign also touched upon Moldova during its parliamentary elections. In this case, Facebook's analytical service revealed 168 fake accounts which, according to them, were local and had nothing to do with Russia (Gressel, 2019). With the use of the described examples, we can say that Russia manages to covertly manipulate public opinion with disinformation easier in the Eastern Partnership region than in the states of Central and Western Europe. For the Russian Federation, this region is the main sphere of foreign policy influence as well as the main area for improving its hybrid warfare strategies.

Due to the fact that for the European institutions and the member states of the European Union overcoming Russian hybrid warfare seems to be sort of a "mission impossible," it is necessary to use the resources possessed by the Eastern Partnership region. By using coordinated strategic approaches,

it is possible to effectively, if not completely, deal with the anti-Western narratives. It is of vital importance for the European Union to support organizations and initiatives such as the Media Reform Center in Ukraine. This organization implements educational programs for establishing Western journalistic standards. In addition, the main field of research of the organization is disinformation and propaganda, informing the international community of the negative purposes of fake news through articles and statistical data. The organization runs an electronic platform (www.stopfake.org) which makes unmasking sources and artificially concocted stories of the anti-Western narrative more accessible for the international audience (Stop Fake, 2020).

With technological progress, the role and principles of information warfare have changed as well. Since using "soft power" and propaganda strategies may be much more effective than projecting military power, it is necessary to make changes to Europe's defense and security strategy in terms of its Eastern dimension. Given the reality of Russian hybrid warfare, expanding the Eastern Partnership program along the lines of cyber security will turn the European Union into a powerful geopolitical player on an international level. Cooperation in the fields of security and defense in this region will enable the European Union to develop technologies and react rapidly to the transformed elements of Russian hybrid warfare.

Conclusion and Recommendations

It is possible that we will not be able to access the strategic depths of Russian hybrid warfare; however, as Karl Haushofer states, in terms of geopolitics and in this case – geopolitical Europe, we may have relevant forecasts about Russia's anti-Western plans. Developing cyber security, as well as overcoming barriers erected by disinformation, envisages holistic and constructive approaches on the European continent. The importance of the Eastern Partnership format in opposition to Russian anti-Western information warfare must once again be underlined as the abovementioned region is the primary target of Russia's political and propagandist influences. It is necessary for the European Union to take steps on political, digital and diplomatic fronts in order to overcome Russian hybrid warfare. Therefore, such a strategy requires various types of actions by the member states of the European Union as well as the members of the Eastern Partnership format:

- The European Union requires a unified approach for developing the Eastern Partnership format. It is necessary not to update but, rather, upgrade this format.
- It is necessary to finally establish inclusivity and differentiation in the EaP format which will enable the associated members to receive more benefits by cooperating with the European Union. Therefore, it is necessary to create a common defense format under the conditions of differentiation which will include dealing with anti-Western propaganda, combating disinformation and developing cyber security (Gogolashvili, 2018).
- It is important for the European Union to create a common legal standard for dealing with disinformation which would include sharing and the implementation of standards from the Eastern Partnership format.
- It is necessary to enhance financial and technical support to ENISA and Europol, also creating new mechanisms for strengthening cyber security.
- It is necessary to bolster the European Union's diplomatic corps with the aim of forming a new "cyber alliance," both with the international organizations (NATO, UN) as well as strategic partners (USA, Australia, Canada, Japan).
- The associated partners of the European Union must bring to the agenda the issues of digital security and strategic cooperation. They must openly express readiness to approximate with the European Union in terms of security and defense.

* * *

"We have a long way to go, but there is now an increased momentum to strengthen our collective capacity for action on security and defense" – Josep Borrell, 2020 (European External Action Service, 2020).

Bibliography

- Barigazzi, J. (2019, 10 19). “Borrell urges EU to be foreign policy ‘player, not the playground.’” Brussels, Belgium. Retrieved from https://www.politico.eu/article/on-foreign-policy-josep-borrell-urges-eu-to-be-a-player-not-the-playground-balkans/
- Bulckaert, N. (2018, 07 17). “How France successfully countered Russian interference during the presidential election.” Paris, France. Retrieved from https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/
- Elliott, J. K. (2018, 06 09). “Theatricality and deception: How Russia uses ‘maskirovka’ to shake the world.” Canada. Retrieved from https://globalnews.ca/news/4260938/russia-strategy-maskirovka-military-politics-putin/
- Ellyatt, H. (2020, 07 21). “UK intelligence report says Russia is a capable cyber actor and its influence is the ‘new normal.’” New York, U.S.A. Retrieved from https://www.cnbc.com/2020/07/21/uk-report-says-russia-meddled-in-scottish-referendum.html
- *EU Cyber Direct*. (2019, 11 20). Retrieved from https://eucyberdirect.eu/: https://eucyberdirect.eu/content_knowledge_hu/cyber-related-pesco-projects/
- European Commission. (2019). *Ursula von der Leyen - Mission letter.* Brussels: European Union. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/president-elect_von_der_leyens_mission_letter_to_oliver_varhelyi.pdf
- European External Action Service. (2020, 06 21). *EEAS Europe*. Retrieved from www.eeas.europe.eu: https://eeas.europa.eu/headquarters/headquarters-homepage/81247/europe-security-and-defence-way-forward_en
- European Parliament. (2019). *Online disinformation and the EU’s response.* Brussels: European Union. Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf
- European Parliament. (2020). *The von der Leyen Commission’s priorities for 2019-2024.* Brussels: European Union. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646148/EPRS_BRI(2020)646148_EN.pdf
- Gearóid Ó Tuathail, S. D. (2003). *The Geopolitics Reader.* New York: Taylor & Francis e-Library. Retrieved from https://frenndw.files.wordpress.com/2011/03/geopol-the-geopolitics-reader.pdf
- Gerasimov, C. (2020). “An Eastern Policy Update, but No Upgrade.” *German Council on Foreign Relations*, 2-9. Retrieved from https://dgap.org/sites/default/files/article_pdfs/DGAP-Policy%20Brief-2020-05.pdf
- Gogolashvili, K. (2018). *www.gfsis.org*. Retrieved from https://www.gfsis.org/files/library/pdf/English-2651.pdf
- Gressel, G. (2019, 06 01). PROTECTING EUROPE AGAINST HYBRID THREATS. Berlin, Germany.

- Kakha Gogolashvili, V. P. (2019). *Hybrid Threats in EaP Countries: Building a Common Response.* Tbilisi, Chisinau, Kyiv, Erevan, Brussels. : Georgian Foundation for Strategic and International Studies.
- Pawlak, E. M. (2017). *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?* Brussels: European Union Institute for Security Studies (EUISS). Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf
- Roberts, J. Q. (2015). "Maskirovka 2.0: Hybrid Threat, Hybrid Response." *Joint Special Operations University*, 1-24. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/1007494.pdf
- Špalková, V. (2018). *INFLUENCE OF RUSSIAN DISINFORMATION OPERATIONS: SPECIFIC EXAMPLES IN DATA AND NUMBERS.* Prague: Hanns Seidel Foundation. Retrieved from https://www.europeanvalues.net/wp-content/uploads/2019/02/Influence-of-Russian-Disinformation-Operations-Specific-examples-in-data-and-numbers.pdf
- Stafford, T. (2016, 10 26). "How liars create the 'illusion of truth.'" London, England. Retrieved from https://www.bbc.com/future/article/20161026-how-liars-create-the-illusion-of-truth
- *Stop Fake*. (2020, 09 04). Retrieved from www.stopfake.org: https://www.stopfake.org/en/main/
- Todd C. Helmus, E. B.-B. (2018). Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. Santa Monika, California, U.S.A: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf
- *U.S. Embassy in Georgia*. (2020, 10 01). Retrieved from www.ge.usembassy.gov: https://ge.usembassy.gov/u-s-embassy-statement-on-september-1-2020-cyberattack-against-georgian-ministry-of-health/?fbclid=IwAR2BRVtUZu8Yrgr2Gj-IrnSBT4al-EBjgLmJG3t-ZmWvZAHYmJca_rLUS4s#.X1FI1L_ovcI.facebook
- Vowell, C. J. (2015). *RealClear Defense* . Retrieved from realcleardefense.com: https://www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html
- Weiss, P. P. (2014). "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money." *The Interpreter*, 14-30. Retrieved from https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf