HYBRID THREATS AND THE TRANSFORMATION OF THE STATE POLITICAL INSTITUTE: A NEO-INSTITUTIONAL APPROACH

[a]IGOR V. TKACHUK, [b]ROMAN S. SHYNKARENKO, [c]OLEKSANDR S. TOKOVENKO, [d]STEPAN D. SVORAK, [e]ALINA V. LAVORYK

[a]Scientific Research Institute of Informatics and Law of the Nals of Ukraine, 21030, 35A, Yunost Avenue, Vinnytsia, Ukraine.
[b,c]O. Honchar Dnipro National University, 49005, 72, Gagarin Avenue, Dnipro, Ukraine.
[d]Vasyl Stefanyk Precarpathian National University, 76018, 44a, Shevchenko Str., Ivano-Frankivsk, Ukraine.
[e]King Danylo University, 76018, 35, Konovaltsia Str., Ivano-Frankivsk, Ukraine.
E-mail: [a]ivt7777@gmail.com, [b]romeodz08@gmail.com, [c]kafpol@ukr.net, [d]profesor_ssd_@ukr.net, [e]alina.hurkova@ukd.edu.ua

Abstract: Hybrid expansion on the information space is spreading, there is no reason to believe that hybrid threats are declining. Hybrid aggression is growing, threatening the political security of democracies. The article reviews hybrid influences and threats. The study focuses on the most influential player – the Russian Federation, which poses one of the greatest hybrid threats to states, ignoring the generally accepted civilizational norms of behavior, rules and morals. The factual data were collected and analyzed for the period of 1988–2020 and covered a number of hybrid threats, methods of distribution, methods of implementation, social media used and proven facts. The study focused on the most influential hybrid threats, including propaganda, cyber attacks, hybrid wars and discrediting government agencies.

Keywords: propaganda, cyber attack, hybrid war, political parties, methods and ways of hybrid attacks.

1 Introduction

The rapid development of information technologies in the late twentieth and early twenty-first century has become not only a positive factor, but at the same time has had catastrophic consequences for modern society. Information warfare has become the most important lever of hybrid war, in which zombie reality becomes threatening, becomes an efficient tool of politics, distorts the political institutions of states and turns the opponent into an enemy (Fridman et al., 2019).

Mankind has encountered a new phenomenon – hybrid warfare (Hoffman, 2011), which combines traditional methods of war with non-traditional ones. In an “undeclared” hybrid war the aggressor uses Special Forces, irregular armed groups, supports internal conflicts and separatist movements, and successfully uses all the tools of propaganda, diplomatic measures, cyber attacks, and economic pressure (Caliskan, 2019). In addition, hybrid threats pose a particular threat, as the enemy is able to use a coordinated range of different resources through diplomatic, military, intelligence and economic influence by distorting information and imposing its own distorted reality (Giegerich, 2016). Deadly and destructive attacks can be launched and carried out instantly from distant places, leaving no trace to determine their origin (Stoker, 2016). Hybrid attacks are not only a tool of asymmetric or non-state players. An important role, unfortunately, is played by totalitarian state structures (Cox et al., 2012).

The greatest threat to the stability and democracy of political institutions is posed by states with a totalitarian regime, in which formal state institutions do not play a significant role. Dominant in such destructive regimes is the neo-institutional approach in the political sphere, in which political institutions are treated through the prism of the relationship between formal norms and informal rules of the game (Andress & Winterfeld, 2011; Lazaridis et al., 2016).

The Russian Federation is an example of a state in which generally accepted models of democratization show their incompleteness and insufficiency. The Kremlin uses the full range of its government bodies to advance its foreign policy abroad in a rather aggressive manner, using all means of hybrid warfare: propaganda, espionage, sabotage, cyber-attacks and military intervention (Renz, 2016). It should be noted that Russia’s hybrid policy is characterized by a systematic and coordinated nature, the main purpose of which is to discredit and undermine the democratic values of Western society, to transform and distort the European political system (Treisman, 2018).

The aim of this study was to highlight the most significant hybrid threats, challenges and consequences they bring. The article analyzes the means and methods by which hybrid attacks have been successfully implemented, as well as the impact they have had on the political institutions of countries that have undergone the hybrid influence. Emphasis is placed on the neo-institutional approaches of individual states, which cause a hybrid threat to the political institutions of democratic countries.

2 Methods

2.1 Data Sources

The most significant hybrid threats and all the challenges they pose to the stability and democracy of political institutions have been selected for this study. Such hybrid threats include: propaganda, cyber attacks, hybrid wars, discrediting government agencies. Table 1 details the discussed in the article tools through which hybrid attacks were carried out, as well as the methods of their implementation.

Table 1. The list of researched hybrid threats, methods of distribution and ways of their implementation

Hybrid threats	Methods of distribution	Methods of implementation	Used social media / Proven facts
Propaganda	Television and radio	Information manipulation and disinformation through television and radio	Russia Today, Sputnik, China Daily, Press TV, TRC
	Digital platforms	Creating provocative Facebook pages	“Blacktivist”, “Being Patriotic”, “Secured Borders”,“Texas Rebels”
	Blogs and sites	Dissemination of false information	ZeroHedge.com referral network
Cyber attacks	Internet	Disconnect from the Internet	2007 - Estonia: the work of all state institutions is paralyzed, 2009 - Kyrgyzstan: US military base is evicted
		Intervention into the Internet to coordinate the military actions	2014 - Ukraine: Crimea is occupied by Russia
		Search and retrieve of information	2015 - Germany: attempts to capture data on the work of the Bundestag and NATO, 2016 - USA: penetration to confidential information of the Democratic Party
Hybrid wars	Military conflicts	Direct military support	1988-1994 - Azerbaijan: Armenia’s occupation of seven districts of Azerbaijan and Nagorno-Karabakh with Russian

			support for the Armenian army. The military conflict has become frozen. 2008 - Georgia: Russia's military support for the self-proclaimed republics of South Ossetia and Abkhazia. In 2020 Azerbaijan's army has won back by military means the greater part of this territory
		Introduction of a peacekeeping contingent	1992 – Moldova: Prydnistrovia conflict, bringing in the peacekeeping contingent - the 14th Russian Army from the territory of Moldova. The military conflict has become frozen
		Annexation of the territory	2014 – Ukraine: Russia annexes the Autonomous Republic of Crimea and the city of Sevastopol. Ukrainian territories are still under occupation
		Indirect military support is disguised as actions of local marionettes	2014 – Ukraine: Russia, using the so-called "green men" and numerous forces of Russian troops, occupied certain areas of Donetsk and Luhansk regions. The military conflict still continues with variable intensity
Discrediting government agencies	Support of loyal political parties	Financial assistance	Parties that help to legitimize the Kremlin's policies and increase Russian disinformation – France: National Front, United Kingdom: British National Party
		Ideological support	Parties that are loyal to the pro-Moscow worldview – Germany: Alternative for Germany, Austria: Freedom, Greece: Golden Dawn, Hungary: Jobbik, Italy: Northern League, Belgium: Vlaams Belang

Information on the impact of propaganda was obtained from a number of sources, including: social media, digital platforms, blogs and sites (Bugayova & Barros, 2020; Helmus et al.,2018). With regard to cyber attacks carried out via the Internet, the following data were used to cover individual cyber attacks: disconnection from the Internet (Synovitz, 2009; Traynor, 2007). interference in the Internet to coordinate the military actions (Kofman et al., 2017), search and retrieval of information (BBC News, 2016; Hamburger & Tumulty, 2016). To analyze the devastating effects of the hybrid wars that caused the frozen military conflicts, the following sources have been developed that demonstrate different ways of waging a hybrid war, including: direct military support (Allison, 2009; BBC News, 2020) bringing in the peacekeeping contingent (Treisman, 2018; Helmus et al., 2018), annexation of the territory (Matveev et al., 2009) indirect military support disguised as local marionettes. (Antonyuk & Malskyy, 2016) Information on discrediting government structures by supporting political parties was obtained from a number of sources (Lazaridis et al., 2016; Kramer & Speranza, 2017).

2.2 Analytical Approach

This research is based on data that indicated hybrid threats and their impact on the transformation of political institutions of states, as well as the role of informal institutions in political processes. A number of theoretical research methods were used and combined in the work: historical and logical methods, analysis, synthesis, classification, comparison, generalization and analogy, induction and interpretation. The methodological basis of the study consists of documents and published factual or statistical data that demonstrate the speed of political events and directly cover issues of hybrid threats, including disinformation, its global impact and potential consequences for the political systems of individual states, Internet intervention and governance, military hybrid interventions and threats that occurred within the time period of 1998–2020.

3 Results

3.1 Consequences of the Influence of Propaganda

Let us consider methods of disseminating propaganda through a number of information sources, among which the most efficient are television, radio, digital platforms, blogs and websites.

One of the most influential means of propaganda of Russian policy on the European continent and in the United States is the massive offensive propaganda by the powerful Russian foreign-language speaking companies Russia Today and Sputnik, which effectively promote Russian ideology and the concept of "Russian world". Russia Today and Sputnik started their activities at the beginning of the XXI century and today these media are located in 100 countries around the world and are presented in 30 languages. This allows Russia to completely manipulate public opinion, destabilize civil society and encourage Western citizens to question the veracity or impartiality of the news they receive from state social media. Similar tactics of information manipulation is inherent in some TV channels, among which we can distinguish the Chinese TV channel China Daily, the Iranian Press TV and the Turkish radio and television corporation TRC.

To overcome hybrid threats for the political institutions of Western countries, the European Commission at the end of 2018 drew up an action plan against false propaganda and disinformation. The plan had four components: 1 – to improve the capacity of European Union institutions to reveal, analyze and detect disinformation; 2 – to coordinate and strengthen the joint response to disinformation; 3 – to mobilize the private sector to combat disinformation; 4 – to raise public awareness of manipulative propaganda and to increase society's resilience to disinformation.

One of the important and efficient means of manipulation is digital platforms, which include a number of social networks, among which an important role is played by Facebook, Twitter, Instagram, Messaging apps, YouTube. To analyze the spread of strategic political propaganda, let us consider the example of one important social platform – Facebook. A rather important tool of Russian propaganda in the United States is the creation of dozens of Facebook pages aimed at shaking the political institution of the state by dividing society into different social groups and inciting racial, religious and political hatred. In particular, a page "Blacktivist" was created for the exploitation of racial affiliation, the page "Being Patriotic" was called to form a negative opinion in society about refugees. To create social tension on religious grounds, the page "Secured Borders" was created, which aimed to quarrel Muslims with Christians. The pages that incited citizens to violate the political-administrative division of the United States include "Texas Rebels".

A fairly illustrative example of propaganda that poses a hybrid threat to the political institution of states is the English-language referral network ZeroHedge.com, which includes seventeen blogs and sites: brotherjohnf.com, journal-neo.org, informationclearinghouse.info, thesaker.is, voltairenet.org, veteranstoday.com, stevequayle.com, beforeitsnews.com, endoftheamericandream.com, rense.com, paulcraigroberts.org, goldsilver.com, counterpunch.org, nakedcapitalism.com, globalresearch.ca, washingtonsblog.com, drudgereport.com. ZeroHedge.com is aimed primarily at the American audience. It provides high-quality news for the financial industry and is among the most popular financial blogs in the United States. This allows together with financial news to spread false and loyal to Kremlin policy among a wide range of Internet consumers.

3.2 Consequences of Cyber Attacks

Cyber attacks pose a significant threat primarily to the national security of the state, its constitutional values and the rule of law. Cyber espionage is mostly aimed at stealing commercial developments, especially in the aerospace and communications industries. A special threat is posed by the cyber attacks of the political nature of the Russian secret services, whose actions are aimed at exerting pressure or influencing the course of political events in a particular country, especially with the aim of falsification of elections in a number of Western countries. To demonstrate the impact of cyber attacks on the stability of political institutions we present a number of examples of cybercrime during 2007-2016.

One of the methods of cyber attack aimed to punish governments for certain political acts that Russia did not like was to temporarily disconnect from the Internet, which paralyzed the work of all governmental agencies. In particular, in 2007 such a cyber attack took place in Estonia as punishment for the intention to move the Russian World War II memorial and the graves of Russian soldiers.

Among the effective cyber attacks of the Russian secret services is the hacker attack in 2009, which caused the closure of two of the four Internet providers in Kyrgyzstan. The president of this republic was under pressure to evict a US military base. The goal was achieved. In addition, after the closure of the military base in Kyrgyzstan, $ 2 billion were provided as aid and loans from the Kremlin.

One of the largest cyber attacks carried out by Russian special services took place in 2014. Interference with the Internet in Ukraine has allowed the Russian government to coordinate the military actions, invade of pro-Russian insurgents armed by Russia, and take control of Crimea.

In 2015, a large-scale hacker attack was carried out against the German Bundestag computer network. The purpose of the intrusion was to search for information that concerned not only the work of the Bundestag, but also information about the leaders of Germany and NATO.

Examples of cybercrime to influence elections in democratic countries include Russian hackers' intrusion into Democratic Party information servers and gaining access to personal emails of the Party's officials to discredit presidential candidate Hillary Clinton.

3.3 Consequences of the Influence of Hybrid Wars

In the late twentieth century, after the collapse of the Soviet Union, Russia launched a series of hybrid wars within the post-Soviet space, characterized by the use of irregular armed groups, local criminal groups and regular Russian armed forces. However, the Kremlin, while officially denying its involvement in armed conflicts, did not formally bear any legal responsibility for the aggression committed against a number of states. Let us consider military conflicts that have the features of a hybrid war and were initiated by Russia since more than 30 years ago.

The first military conflict supported by Russia on the part of Armenia should be attributed to the territorial division of Nagorno Karabakh between the Muslim state Azerbaijan and the Christian country Armenia. As a result of the Armenian-Azerbaijan war of 1988–1994 Armenia took control, apart from Nagorno-Karabakh, of the territory of seven Azerbaijan districts around it. Together with Karabakh, they make up 20% of Azerbaijan's territory within its internationally recognized borders. This conflict continues till present. Despite the fact that the UN adopted four resolutions in 1993 recognizing the occupation of seven districts by Armenia, Nagorno-Karabakh during a long time had an uncertain status, a buffer zone controlled by the Armenian army. Without the Russia's direct support of the Armenian army this military conflict would not have acquired the status of a frozen one. In 2020 Azerbaijan's army has won back by military means the greater part of this territory.

The second hybrid aggression, the so-called Prydnistrovian conflict, began in 1992. It was an armed confrontation between Moldova and Prydnistrovia encouraged by Russia after Moldova gained independence and sovereignty from the Soviet Union. At that time, there were several units of the 14th Russian Army, which Moscow quickly "retrained" as "peacekeepers". Despite Russia's commitment during the 1999 OSCE Istanbul Summit to withdraw its 14th Army from Moldova by 2001, it has not kept its promises. The conflict still remains unresolved.

The third military aggression in terms of hybrid war is the events in Georgia in 2008. Russia then acted as a peacemaker on the side of the self-proclaimed republics of South Ossetia and Abkhazia, immediately after the end of the military actions. The Kremlin has supported the state independence of South Ossetia and Abkhazia, taken over the financial support of these Georgian regions, and established military bases on their territory. Without Russia's open aggression against Georgia in 2008 and its support of the self-proclaimed leaders of Abkhazia and South Ossetia, Georgia would not have lost 20% of its territory, and the frozen military conflict would not still exist.

Without incurring any punishment from the international community for the military aggressions in the Caucasus and Moldova during 1999–2008, Russia decided to start its largest hybrid war in early 2014, which aimed to block Ukraine's European and Euro-Atlantic course and return it to the sphere of the Russian influence. In February 2014, the Russian Federation, violating the norms and principles of international law as well as bilateral and multilateral agreements, annexed the Autonomous Republic of Crimea and Sevastopol. The next step was a covert hybrid war in the Donbas, in which Russia used military "special forces" of so-called "green men", intelligence officers and numerous forces of Russian troops disguised as local Russian marionettes to occupy parts of Donetsk and Luhansk regions. Like the above-mentioned three hybrid wars launched by the Russian Federation, the hybrid aggression against Ukraine with the steady Kremlin's participation has turned into a military conflict that lasts till present with variable intensity.

3.4 Consequences of Discrediting State Institutions

European countries also experience hybrid threats from the Russian Federation, which undermine European Union and support the political parties loyal to the Kremlin. The coming to power of anti-system forces in the European Union significantly complicates the looming financial and migration crises and other important problems that weaken the political and economic role of the EU in the world.

For example, Russian banks in France are actively financing the National Front, which through this party's activities legitimizes the Kremlin's policy and intensifies Russian disinformation. The Institute of Democracy and Cooperation (Institut de la democracyie et de la coopération) was established with the same intentions, headed by a former Russian member of parliament. This Institute is working hard to give Russia a positive image in France. The Kremlin is exerting considerable influence on

British public opinion through the British National Party (BNP), which has intensified its political activities in recent years, increasing the number of candidates running in elections and winning more and more seats in local councils.

In addition, there are a number of parties in Europe for which Russia is not responsible, but these parties are loyal to the pro-Moscow worldview. These include far right, such as the Alternative for Germany (AfD), the Austrian Freedom Party (FPO), the Greek Golden Dawn, the Hungarian Jobbik, the Italian Northern League and the Belgian Vlaams Belang (VB). Besides, there are pro-Russian far left parties in Europe, among which the Spanish party Podemos, the Greek Syriza and the German Die Linke are particularly loyal to the Kremlin's policies. Each of these parties has its own ideological platform, but what they have in common is that the above-mentioned parties support the policies of the Russian Federation and defend the Kremlin's interests. Some of them are skeptical about the future of the European Union thus destabilizing the European politics and European democratic values.

4 Discussion

Hybrid threats in today's world are gaining a dangerous scope and demonstrate that targeted hybrid aggression can destabilize not only regional but also global security structures (Fridman et al., 2019). Expert research and our data show that democratic societies are particularly vulnerable to hybrid influences, as they profess the values of political pluralism, liberal freedom of speech and meetings, respect for individual rights, the rule of law, tolerance and political correctness (Murray & Mansoor, 2012). At the same time, totalitarian regimes, characterized by a lack of rule of law and the predominance of informal institutions, use aggressive hybrid expansion against democratic states, disregarding generally accepted civilizational norms of behavior, rules and morals (Helmke & Levitsky, 2004).

According to author (Treisman, 2018) and our research, the Russian Federation poses one of the greatest hybrid threats not only to a number of political institutions in the post-Soviet space, but also to European states and the United States. As it is shown in Table 1, one of the important resources used by Russia and Kremlin-loyal states and regimes is offensive propaganda through a range of media available to the general public – television and radio, various digital platforms, blogs and sites. (Renz, 2016; Babiker et al., 2019). The lack of censorship in liberal Western democracies creates insecurity and vulnerability of the society to the onslaught of disinformation and false propaganda (Bradshaw & Howard, 2018).

Cyber attacks are one of the new hybrid threats associated with information technology. The aggressor has the potential to carry out vicious attacks in cyberspace, often leaving an undetected both the source of cybercrime and the perpetrator or group of criminals (Andress & Winterfeld, 2011). As our research has shown, a number of cyber attacks carried out under the leadership of the Kremlin have been successful and have caused significant damage to individual states. In particular, the largest cyber attack carried out by Russia led to the capture and annexation of Ukrainian territories – Crimea and the city of Sevastopol. In addition, the number of cyber-attacks on Western democratic states aiming to seize secret information or spread disinformation has increased in recent years (Hoffman, 2011).

Table 1 shows a number of successful hybrid wars waged by the Russian Federation during 1988-2014. These military conflicts remain frozen or continue to vary in intensity. They have had devastating consequences of unprecedented human, territorial and economic losses for states, which underwent hybrid expansion, and demonstrate the vulnerability of Western democracies to the Kremlin's forceful hybrid policies.

The West's unpreparedness for cyber threats by Russia, discrediting government agencies also has disastrous consequences. With the active support of parties loyal to the Kremlin's policies the Russian Federation is exacerbating a number of problems and challenges posed by Brexit, the financial and migration crises in Europe and is undermining European unity (Lavenex, 2016).

Thus, neo-institutionalism, which is primarily the product of the political system of states with undemocratic values, poses serious challenges and threats to developed liberal democracies. Analyzing the hybrid threats and their consequences, it should be noted that hybrid aggression not only led to the escalation of conflicts on the European continent, but also resulted in transformation of political institutions in many countries, shaking the decades-old democratic achievements of society.

5 Conclusions

Hybrid threats have gained dangerous scope in today's world. Due to information technologies the tools with which they are embodied have become sophisticated and comprehensive. As our research has shown, the greatest threat to the stability and democracy of political institutions within the post-Soviet space and in the Western countries is the Russian Federation. The Kremlin is using all possible means of hybrid expansion to discredit and undermine the democratic values of Western society. In particular, these include propaganda, which allows to strongly manipulate public opinion and to destabilize civil society, encouraging citizens to doubt the veracity or impartiality of the news they receive from state information sources. A significant threat is posed by political cyber attacks used by Russian intelligence services to pressure or falsify elections in a number of Western countries, as well as by financial and propagandist support for political parties loyal to the Kremlin.

The largest hybrid aggressions that have shaken the political institutions of states include a series of hybrid wars that have taken place over the last 30 years within the post-Soviet space and have been characterized by the use of irregular armed groups, local criminal groups, and regular Russian armed forces.

Summing up the research, it should be noted that hybrid threats and direct expansion are among the most important challenges of today, which destabilize the political institutions of democratic countries. Overcoming hybrid threats requires the unity and coordination of Western countries. The European Commission has taken a number of successful steps in this direction.

Literature:

1. Allison, R. (2009). The Russian case for military intervention in Georgia: international law, norms and political calculation. *European Security,18*(2), 173-200.
2. Andress, J, Winterfeld, S. (2011). *Cyber warfare: techniques, tactics and tools for security practitioners.* Amsterdam: Elsevier.
3. Antonyuk, N., Malskyy, M. (2016). Russia's hybrid warfare against Ukraine in the context of European Security. Visnyk of the Lviv University. *Series International Relations, 38,* 23-42.
4. Babiker, M., Karaarslan, E., Hoşcan, Y. (2019). A hybrid feature-selection approach for finding the digital evidence of web application attacks. *Turkish Journal of Electrical Engineering and Computer Sciences, 27*(6), 4102-4117.
5. BBC News [Interner]. (2016). Russia' Was Behind German Parliament Hack. Available from: https://www.bbc.com/news/technology-36284447
6. BBC News [Internet]. (2020). Armenia, Azerbaijan and Russia Sign Nagorno-Karabakh Peace Deal. Available from: https://www.bbc.com/news/world-europe-54882564
7. Bradshaw, S., Howard, P. (2018). The global organization of social media disinformation campaigns. *Journal of International Affairs, 71*(15), 23-32.
8. Bugayova, N., Barros, G. (2020). *The Kremlin's Expanding Media Conglomerate.* Available from: http://www.understandingwar.org/backgrounder/kremlin%E2%80%99s-expanding-media-conglomerate
9. Caliskan, M. (2019). Hybrid warfare through the lens of strategic theory. *Defense and Security Analysis, 35*(1), 40-58.
10. Cox, D.G., Bruscino, T., Ryan, A. (2012). Why hybrid warfare is tactics not strategy: a rejoinder to "future threats and strategic thinking. *Infinity Journal, 2*(2), 25-29.

11. Fridman, O., Kabernik, V., Pearce, J.C. (Eds.). (2019). *Hybrid conflicts and information warfare: new labels, old politics.* Boulder: Lynne Rienner.
12. Giegerich, B. (2016). Hybrid warfare and the changing character of conflict. *Connections: The Quarterly Journal, 15*(2), 65-66.
13. Hamburger, T., Tumulty, K. (2016). WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations. Available from: https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/
14. Helmke, G., Levitsky, S. (2004). Informal institutions and comparative politics: a research agenda. *Perspectives on Politics, 2*(4), 725–740.
15. Helmus, T.C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., … Winkelman, Z. (2018). *Russian social media influence: Understanding Russian propaganda in Eastern Europe.* Santa Monica: RAND Corporation.
16. Hoffman, F.G. (2011). Future threats and strategic thinking. *Infinity Journal, 4*(Fall), 17-21.
17. Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., Oberholtzer, J. (2017). *Lessons from Russia's operations in Crimea and Eastern Ukraine.* Santa Monica: RAND Corporation.
18. Kramer, F.D., Speranza, L.M. (2017). *Meeting the Russian hybrid challenge. A comprehensive strategic framework.* Washington DC: Atlantic Council.
19. Lavenex, S. (2016). Multilevelling EU external governance: The role of international organizations in the diffusion of EU migration policies. *Journal of Ethnic and Migration Studies, 42*(4), 554-570.
20. Lazaridis, G., Campani, G., Benveniste, A. (Eds.). (2016). *The rise of the far right in Europe: populist shifts and "othering"*. London: Palgrave Macmillan.
21. Matveev, D., Selari, G., Bobkova, E., Cseke, B. (Eds.). (2009). *Moldova–Transdniestria: Working together for a prosperous future: Negotiation Process.* Chisinau: Cu drag Publishing House.
22. Murray, W., Mansoor, P.R. (Eds.). (2012). *Hybrid warfare*. Cambridge: Cambridge University Press.
23. Renz, B. (2016). Russia and hybrid warfare. *Contemporary Politics, 22*(3), 283-300.
24. Stoker, D. (2016). What's in a name II: "Total War" and other terms that mean nothing. *Infinity Journal, 5*(3), 21-23.
25. Synovitz, R. (2009). Kyrgyz Eviction Warnings Intensify Over U.S. Air Base. Available from: https://www.rferl.org/a/Kyrgyz_President_Threatens_To_Kick_US_Troops_Out_Of_Air_Base/1379212.html
26. Traynor, I. (2007). Russia Accused of Unleashing Cyberwar to Disable Estonia. Available from: https://www.theguardian.com/world/2007/may/17/topstories3.russia
27. Treisman, D. (Ed.). (2018). *The new autocracy: Information, politics, and policy in Putin's Russia*. Washington DC: Brookings Institution Press.

Primary Paper Section: A

Secondary Paper Section: AG