Pomianowski Piotr, Maćkowiak Ewa. 2012. „Zwalczanie finansowania terroryzmu w świetle prawa obowiązującego w Polsce i we Francji". Przegląd Bezpieczeństwa Wewnętrznego : 71-94.

Stefański Ryszard Andrzej. 2000. Przestępstwa przeciwko bezpieczeństwu w komunikacji, Warszawa: C.H. Beck.

Warylewski Jarosław. 2015. Prawo karne. Część ogólna, Warszawa: LexisNexis.

Wojciechowski Janusz. 1997. Kodeks karny. Komentarz, Warszawa: Librata.

Zoll Andrzej. 1999. Kodeks karny. Część szczególna, T.2, Komentarz do art. 117-277, Warszawa: Wolters Kluwer.

Tymur ANDRIYEVSKYY[1]

Department of Political Science, Sociology and Culturology

G. S. Skovoroda Kharkiv National Pedagogical University[2]

Kharkiv, Ukraine

andrievskytimur@gmail.com

THE PURPOSES OF THE RUSSIAN-UKRAINIAN HYBRID WAR

ABSTRACT: The aim of the article is to present the idea that Russian-Ukrainian hybrid war influences the world order and international relations. It also points to the fact that Russia exploits new digital technology in this conflict. Furthermore, the article emphasizes the use of fake news, propaganda, interference in the election processes and cybernetic attacks that are a new weapon of the new generation warfare – hybrid war or war of the information society. Moreover, the author describes the activities that Russian Federation has undertaken in Estonia since 2007 and it also illustrates the purpose of Russian aggressive measures. The author makes an attempt to prove that the main purpose of Russian-Ukrainian hybrid war is to create chaos, undermine the values of the democratic world and cultivate a comprehensive atmosphere of mistrust and nihilism. Additionally, it is stated that the aggressor uses the very institutes of democracy and their weaknesses as a weapon.

KEYWORDS: war, hybrid war, Russian-Ukrainian war, fake news, propaganda, undermining technologies, informational operations

CELE ROSYJSKO-UKRAIŃSKIEJ WOJNY HYBRYDOWEJ

ABSTRAKT: Celem tego artykułu jest zaprezentowanie, że rosyjsko-ukraińska wojna hybrydowa wpływa na ład światowy i stosunki międzynarodowe. Wskazuje również na fakt, że Rosja wykorzystuje w tym konflikcie nowe technologie cyfrowe. Ponadto artykuł podkreśla wykorzystanie fake news, propagandy, zakłóceń w procesach wyborczych i ataków cybernetycznych, które są nową bronią w wojnie nowej generacji – wojnie hybrydowej lub wojnie społeczeństwa informacyjnego. Ponadto Autor opisuje działania, które w Estonii od 2007 prowadzi Federacja Rosyjska i prezentuje środki agresywnych rosyjskich działań. Autor podejmuje również próbę wykazania, że głównym celem rosyjsko-ukraińskiej wojny hybrydowej jest stworzenie chaosu, podważenie wartości demokratycznych na świecie i pielęgnowanie atmosfery nieufności i nihilizmu. Ponadto stwierdza, że agresor wykorzystuje jako broń instytutucje demokratyche i ich słabości.

KEYWORDS: wojna, wojna hybrydowa, wojna rosyjsko-ukraińska, fake news, propaganda, osłabienie technologii, operacje informacyjne

[1] Graduate student in G.S. Skovoroda Kharkiv National Pedagogical University, Department of Political Science, Sociology and Culturology, Ukraine. Master of laws.

[2] Харьковский национальный педагогический университет имени Сковороды.

INTRODUCTION

The Russian-Ukrainian hybrid war has lasted for almost full four years. The achievements of the aggressor during this war were the annexation of the Autonomous Republic of Crimea and the formation of "puppet" governments in some districts of Donetsk and Luhansk regions that are effectively controlled by the Russian administration. In general, according to the preliminary findings of the Prosecutor of the International Criminal Court, this conflict has all signs of international armed conflict between Ukraine and the Russian Federation[3]. Therefore, fewer reasons are left to consider this conflict as internal. We have to admit that this is aggression, an international crime punishable by the international community.

However, the question arises: were these losses of the territory of Ukraine (in proportion to the entire territory of the state, according to the words of the President of Ukraine P. Poroshenko, is about 7%) the real purpose of Russian aggression? Definitely not. The main objective of Russian aggression, in the author's opinion, is to prevent Ukraine from coming out of Russia's sphere of influence, to fight against Ukraine's right to its own sovereignty and against its right to resolve independently its own political destiny. Russia's geopolitical ambitions that are leading to the confrontation have been well explained by President Putin's words - he called the collapse of the USSR "the greatest geopolitical catastrophe of the twentieth century".

The ongoing Russian-Ukrainian hybrid war has no analogues in world history. Indeed, some elements have already been used before, but the combination of all the methods, especially non-military, each day complements or changes the concept of the hybrid warfare. The main battlefronts are transferred from the real battlefields to completely different spheres: economics, domestic and foreign policy, international relations. Of course, history proves that there have already been the cases when the war became global for all spheres of the state's life, but the unique phenomenon of the present warfare is the fact of exploiting precisely all the methods and mechanisms in which ordinary citizens (non-combatants) become victims of an aggressor or become aggressor's weapon themselves.

Consequently, in this article, the author is going to consider the goals pursued by the aggressor and the methods by which he intends to achieve the benefits. The conclusions obtained in the analysis should help us to formulate the concept of effective counteraction to aggression in the information society in the future as well as to prepare for new challenges, since the methods that have been discovered could be applied not only by Russia, but also by terrorist organizations, radical Islamists and other actors.

[3] International Criminal Court. The Office of the Prosecutor. Report on Preliminary Examination Activities 2016, p. 35 § 158 W https://www.icc-cpi.int/iccdocs/otp/161114-otp-rep-PE_ENG.pdf .

THE PURPOSES OF HYBRID WARFARE: UNDERMINING THE DEMOCRACY AND DISORDER

Unfortunately, in the Russian-Ukrainian hybrid war, Ukraine has been given the role of the hot spot, the main military front and the testing ground for new instruments and methods of the new generation warfare. Using the concept of the "Russian-Ukrainian hybrid war", the author relies on the works of national security researchers from the National Institute for Strategic Studies of Ukraine – one of the first to put this concept into Ukrainian scientific circulation[4].

However, the conflict itself is increasingly taking on the features of the global confrontation of two worlds fundamentally different in their value orientations. The sanctions imposed on the Russian Federation by the world's democratic community after the annexation of the Autonomous Republic of Crimea and the invasion on the Donbas are a common preventing element of deterring an aggressor that are applied by a civilized society. However, for Russia (in the understanding of its leaders), all the sides of the Western world, that support the sanctions regime against it, automatically become the party of the conflict. The West must understand that Russia (in its conviction) has not been fighting against only Ukraine for a long time. Russia fights with the whole world, where its "values" are not accepted.

Sanctions themselves are a deferred destructive factor with catastrophic consequences for the Russian economy, so the Kremlin is facing the question of state's survival and preserving the current model of governance along with its political elite.

Avoiding the destructive effects of sanctions to Russia is possible in two ways: civilized - by withdrawing its troops from the occupied territories, conducting investigations of the relevant war crimes and covering the damages inflicted in Ukraine. However, the analysis of recent events confirms that the second, Soviet way of the Cold War was actually chosen to solve the problem of breaking the democratic systems in the West, weakening Western states from the inside, creating a so-called "controlled chaos" to achieve complete destabilization of political processes. Under such conditions, Russia hopes to start bargaining for the abolition of sanctions and simultaneously tries to maintain its "assets".

Hybrid war is a war of the information society, a new generation of wars, when the territory does not need to be physically captured, but it is necessary to gain control over people's minds, thoughts and decision-making[5]. Propaganda, information and cybernetic attacks, the creation of alternative reality in the information environment – there are the asymmetric actions of Russia intended to change the worldview of people in democratic states.

---

[4] V. Horbulin and others, *The World Hybrid War: Ukrainian Forefront: monograph*, Kyiv: The National Institute for Strategic Studies, 2017 – p.17, in Ukrainian. (Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017, с. 17) W http://lib.rada.gov.ua/LibRada/static/about/text/HW_druk_fin%2Bsite_changed.pdf

[5] T. Andriyevskyy, Hybrid war: nature and basic strategies, "De securitate et Defensione", No. 1 (3) /2017, pp. 158-166 in Russian (Т. Андриевский. "Гибридная война: сущность и базовые стратегии") W http://www.desecuritate.uph.edu.pl/images/De_Securiatete_et_Defensione_1_3_2017_NUMER_5-1.pdf c.165.

When Ukraine is forced to "physically" restrain Russia's aggression by using its armed forces, the West is increasingly forced to face a new type of intervention - information operations. Therefore, under information operations, the author means the intervention of state or non-state actors in the state's internal policy in order to spread aggressor's beneficial informative narratives using the propaganda, disinformation or information chaos. Unfortunately, digitalization of modern social processes and interactions is very suitable environment for such undermining information operations. Digital globalization blurs the physical boundaries between states, in fact, violating the very sovereignty of the state. And if several decades ago such globalization has been seen exclusively as an element of global progress for simplifying communication between people, spreading knowledge, creating new markets and a new sector of the economy – today these technologies turned into the weapon.

Today we are witnesses of Russia's inferiority complex of imperial past, where Russia is mistakenly seeking the possibility to regain the status of a superpower not by creating a competitive economy, innovations, capable trade, etc., but through aggressive actions, as the USSR once did. The use of subversive technologies during the Cold War was a commonplace phenomenon for the parties 50 years ago. The combination of such subversive measures, including dissemination of deceptive information, using the agents of influence and covert organizations, media manipulations are well described in the analytical report "Active measures" of the USSR against USA: preface to hybrid war" of the National Institute of Strategic researches of Ukraine[6]. However, the West was unprepared for the fact that after the collapse of the USSR, modern Russia decided to use the same measures only with the use of modern technologies.

In general, the Russian authorities firstly tried these technologies on their own society. Monopolizing the power over the media, they built another alternative reality for their citizens, where the West again became the main enemy to Russia. By spreading state control over social networks (VKontakte, Odnoklassniki), Russia began to apply its first fake accounts to form "true" political thoughts among citizens. The monopolized information allowed them to get rid of any political rivals and to neutralize the opposition's attempts to spread its point of view. Such processes, the sources and development of Russian digital propaganda are well described in the monograph by S. Sanovich from New York University[7].

Having formed a stable undemocratic system within the state, Russia has dared to use digital technologies outside the country. Therefore, in 2007, Russia used a massive hacking attack on the government networks of Estonia[8]. All this happened on the background of the

[6] D. Dubov, A. Barovska, T. Isakova, I. Koval, V. Horbulin, "*Active measures" of the USSR against USA: preface to hybrid war: analytical report. Kyiv*, The National Institute for Strategic Studies, 2017, 48 p. In http://www.niss.gov.ua/public/File/book_2017/active___druk_bleed-5.pdf

[7] S. Sanovich. Computational Propaganda in Russia: The Origins of Digital Misinformation. University of Oxford, 2017 In http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Russia.pdf

[8] H. Grassegger, M. Krogerus., *Fake news and botnets: how Russia weaponised the web*, "The Guardian", 02.12.2017 In https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia.

scandal with the transfer of the monument of a Soviet soldier, who is considered to be a symbol of Soviet occupation in Estonia. Furthermore, such measures were used during the Russian invasion in Georgia in 2008. Aggression against Ukraine was also prepared with the use of information operations. It is not surprising that Russia used information attacks before the annexation of the Crimea, but this issue is only beginning to become publicized in the West[9]. Thus, using a network of its propaganda channels such as RT or Sputnik, Russia tried to spread false opinions about the "internal" conflict in Ukraine, to show the Western public that Russia is a friendly and kind country, and the annexation of another state's territory is not a crime. It should be noted that the issue of Ukraine, the use of hacker attacks by Russia, information operations, other subversive activities are only being analyzed and studied. This is a separate topic of another big research.

Due to the fact that the Russian aggression against Ukraine did not become a blitzkrieg, and sanctions slowly strike the state's economy, Russia began to resort to more active actions and as a result the governments of the Western powers and the political systems have already become the target.

Intervention in the presidential elections in the United States was accompanied not only by the direct actions of the Russians. As the latest investigation by Facebook shows, for two years from accounts "allegedly guided by Russia", they bought a political advertisement worth 100 thousand dollars. An internal investigation found that 3000 advertisements and posts were paid from 470 accounts and pages that were not used by real people. The advertising, estimated to be seen from 23 to 70 million people, was not intended to support a particular candidate in the US presidential election[10]. In total, over the past two years 126 million people have seen Russian political advertising[11]. The content of the posts presented controversial social and political messages and affected topics such as LGBT, interracial relations, migration, and the firearms license. The Facebook administration is concerned that the social network has become an element of political confrontation. Conducting the investigation, they are simultaneously looking for ways to counter information operations. The analytical report "Information Operations and Facebook" lists the three main elements that the administration focused on[12]:

---

[9] E. Nakashima., Inside a Russian disinformation campaign in Ukraine in 2014, "The Washington Post", 25.12.2017 In https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html?utm_term=.f64454e2ed36

[10] C.D. Leonnig, T. Hamburger, R.S. Helderman. *Russian firm tied to pro-Kremlin propaganda advertised on Facebook during election*, "The Washington Post", 06.09.2017 In https://www.washingtonpost.com/politics/facebook-says-it-sold-political-ads-to-russian-company-during-2016-election/2017/09/06/32f01fd2-931e-11e7-89fa-bb822a46da5b_story.html?utm_term=.de6206fe1b8e

[11] *Russia-linked posts 'reached 126m Facebook users in US'*, BBC, 31.10.2017 In http://www.bbc.com/news/world-us-canada-41812369

[12] J. Weedon, W. Nuland and A. Stamos, *Information Operations and Facebook. Facebook Inc*., 2017. p. 6 In https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

- Targeted data collection, with the goal of stealing, and often exposing, non-public information that can provide unique opportunities for controlling public discourse.
- Content creation, false or real, either directly by the information operator or by seeding stories to journalists and other third parties, including via fake online personas.
- False amplification, which is defined as coordinated activity by inauthentic accounts with the intent of manipulating political discussion (e.g., by discouraging specific parties from participating in discussion or amplifying sensational voices over others). Facebook administration detected this activity by analyzing the inauthenticity of the account and its behaviors, and not the content the accounts are publishing.

Today, Facebook is trying to improve its network in order to prevent the above risks by[13]:

- Continually studying and monitoring the efforts of those who try to negatively manipulate civic discourse on Facebook;
- Innovating in the areas of account access and account integrity, including identifying fake accounts and expanding security and privacy settings and options;
- Participating in multi-stakeholder efforts to notify and educate at-risk people of the ways they can best keep their information safe;
- Supporting civil society programs around media literacy.

A separate example of Russia's use of bots affecting the political preferences of citizens of other states is Twitter. Account @TEN_GOP was a heavyweight voice on the American far right. It had over 130,000 followers; it was retweeted by some of Trump's aides. When it was suspended, in July 2017, voices across the American far right protested. To some observers, it seemed too good to be true; in October, they were proven right. Twitter confirmed that @TEN_GOP was a fake, run by a Russian operative connected to the notorious "troll factory" in St. Petersburg[14].

All data mentioned above is an example of using new means to destabilize the political system in order to undermine citizens' confidence in political processes, any sources of information, etc. There are strong suspicions that similar attempts to interfere in the electoral process were also carried out against France in the presidential elections of 2017[15], and during so-called Brexit case. Planned information operations use the game on the same sensitive issues (migrants in the EU, Brexit[16], world terrorism, Islam, LGBT rights, etc.), form a single picture of chaos, which is intended to weaken democracy, undermine the faith of people in its values.

[13] *Ibidem*, p.13.
[14] B. Nimmo, *How A Russian Troll Fooled America*, AtlanticCouncil's Digital Forensic Research Lab, 14.11.2017 In https://medium.com/dfrlab/how-a-russian-troll-fooled-america-80452a4806d1.
[15] L. Daniels, *How Russia hacked the French election*, POLITICO, 23.04.2017 In https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.
[16] R. Booth, M. Weaver, A. Hern, S. Walker, *Russia used hundreds of fake accounts to tweet about Brexit, data shows*, "The Guardian", 14.11.2017 W https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.

As for Ukraine, today many finances are spent on Russia's physical deterrence and support of the army. That is why the information sphere remains extremely vulnerable. So, in the political life, in the media, in social networks in Ukraine there are actors who actively promote the new Russian paradigm, which reads: "The enemy is not in the Kremlin, the enemy is in Kiev." These actors use sensitive and painful topics to create a boiling point inside the state for polarizing society, so that people do not trust public institutions. For such manipulations, any good reason is used - from the analogue of the Russian action "immortal regiment" ("Bessmertnyi polk") on the Victory Day over Nazism in the Second World War, to the use of manipulations on the language issue in educational reform, the question of paid medicine in medical reform, etc. Efforts are being made to use the Ukrainian opposition as an "icebreaker" of Ukrainian statehood as such. Not so long ago, the Prosecutor General of Ukraine provided materials on the possibility of financing the "protest actions" in Kiev by the Ukrainian fugitive oligarch Serhiy Kurchenko, who is hiding in Russia (where he has the support of the authorities) and is accused of treason in Ukraine[17].

It is hard to confront all these spectrum of measures taking into account the fact that until the end of the Russia's aggression, in Ukraine Russian television channels are persistently broadcasting, creating in fact their own anti-Ukrainian paradigm. Sociocultural convergence got worse year by year trying to absorb Ukrainian citizens. That is why when the aggression was carried, the aggressor was not identified as an enemy by the great masses of Ukrainians. The separate issue is an attempt to undermine trust to Ukraine among its partners and neighbours. Separate impairment of Ukraine – Poland relationships on the basis of historical memory is the favorable environment for Russia, where Russia predictably will be trying to break up partners and allies. Thus, Polish media themselves published information on the possibility of Russian sponsorship of the groups worsening the relations of the two states by their activities[18].

That is why the specialists of the Hague Centre for Strategic Studies in their analyses "Inside the Kremlin House of Mirrors: how liberal democracies can counter Russian disinformation and societal interference" provide the necessary list of measures to restrain informational aggression and propaganda of Russia[19]. Among the measures these need to be highlighted:

---

[17] *Briefing of the Prosecutor General of Ukraine. Prosecutor General's office of Ukraine*, official website, 05.12.2017. In Ukrainian (Юрій Луценко повідомив, що ГПУ спільно з СБУ виявлено факт фінансування С. Курченком масових акцій протесту у містах України) In https://www.gp.gov.ua/ua/news.html?_m=publications&_t=rec&id=220231&fp=60

[18] P. Andrusieczko, A. Poczobut, M. Wojtczuk, *For the money from Russia in Poland against Ukraine*, "Gazeta Wyborcza", 09.03.2017. In Polish ("Za kasę z Rosji w Polsce przeciw Ukrainie") In http://wyborcza.pl/7,75399,21472245,za-kase-kremla-w-polsce-przeciw-ukrainie.html?disableRedirects=true

[19] S. de Jong, T. Sweijs, K. Kertysova, R.Boshttps., *Inside The Kremlin House Of Mirrors. How Liberal Democracies can Counter Russian Disinformation and Societal Interference*, The Hague Centre for Strategic Studies, 2017, p.65. In https://www.hcss.nl/sites/default/files/files/reports/Inside%20the%20Kremlin%20House%20of%20Mirrors_0.pdf.

1. to invest in social media literacy for the population and for specific segments (civil servants, military people, journalists, bloggers);
2. not to be afraid to close Russian television channels at a favorable opportunity, when they explicitly distribute fake news or propaganda threatening the public;
3. not to repeat Russian narratives and propaganda, use own positive narratives for the population, apply counter-propaganda;
4. not to allow Russia to use the structural problems of society - the government should address these problems;
5. to identify those politicians, representatives of civic organizations, etc., who have permanent contacts with Russia;
6. to spend money on the development of big data analyses to identify those groups that are most vulnerable to Russian disinformation;
7. to understand that Russia is waging a political, non-kinetic war against a civilized world.

Therefore, the author must admit that counteraction to destructive subversive measures is still taking place. While the US is investigating Russia's interference in the elections, the EU already has taken measures thus consolidating the strategy of counteracting the information threat from Russia. European parliament resolution issued in November 2016 states that "the Russian Government is employing a wide range of tools and instruments, such as think tanks and special foundations (e.g. Russkiy Mir), special authorities (Rossotrudnichestvo), multilingual TV stations (such as RT), pseudo news agencies and multimedia services (e.g. Sputnik), cross-border social and religious groups (...) social media and internet trolls to challenge democratic values, divide Europe, gather domestic support and create the perception of failed states in the EU's eastern neighbourhood"[20],

SUMMARY

Thus, the goal of the Russian-Ukrainian hybrid war can be formulated, which is to create chaos, undermine the values of the democratic world and cultivate a comprehensive atmosphere of mistrust and nihilism. This goal extends not only to Ukraine but also to those states that support it. Russia has transformed democracy (which Russia itself does not know) into our enemy. Using the basic values of democracy as a weapon, the aggressor has made it possible for freedom of speech to become a right to lie, freedom to receive information – to freedom to spread fake, lies and propaganda, freedom to peaceful gatherings – to the right to street collisions, and social networks - to a chaotic collection of non-existent individuals to incite hostility. The very idea of democracy is undermined, the very possibility of free, honest and unbiased expression of the person is questionable.

[20] European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)), § 8 In http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0441+0+DOC+XML+V0//EN.

That is why, by categorizing such informational operations depending on their purpose, we can distinguish: 1) operations on the split of a society within the state for its weakening or bringing their own candidates to power; 2) operations to discredit the state on the world stage and for the tensions with its neighbors or partners; 3) operations for the dissemination of general information chaos to achieve individual tactical goals by the aggressor.

That is why one can say that in the face of an active informational confrontation, when the state is trying to be destroyed and captured from within, information-blasting technologies are aimed at the desocialisation of the individual. This person does not trust the authorities for which he/she voted for, does not trust the institutes of democracy, does not trust the media, and does not trust the neighbours. Losing their own values, such a person begins to trust fakes and other people's propaganda. A person pulled out of a normal society, who has lost any value pointers, without his/her own wish becomes the weapon of the enemy. Therefore, right and balanced informational policy should be held, information security, information literacy must be carried on, and it is vital to react timely to new subversive technologies and information traps.

BIBLIOGRAPHY

"Russia-linked posts 'reached 126m Facebook users in US' ". BBC, 31.10.2017 In http://www.bbc.com/news/world-us-canada-41812369.

Andriyevskyy Tymur. "Hybrid war: nature and basic strategies". De securitate et defensione. N 1 (3)/2017 : 158-166 in Russian (Тимур Андриевский. "Гибридная война: сущность и базовые стратегии") .

Andrusieczko Piotr, Poczobut Andrzej, Wojtczuk Michał. "For the money from Russia in Poland against Ukraine". Gazeta Wyborcza, 09.03.2017. In Polish ("Za kasę z Rosji w Polsce przeciw Ukrainie") In http://wyborcza.pl/7,75399,21472245,za-kase-kremla-w-polsce-przeciw-ukrainie.html?disableRedirects=true.

Booth Robert, Weaver Matthew, Hern Alex and Walker Shaun." Russia used hundreds of fake accounts to tweet about Brexit, data shows". The Guardian, 14.11.2017 In https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.

Briefing of the Prosecutor General of Ukraine. Prosecutor General's office of Ukraine, official website, 05.12.2017. In Ukrainian (Юрій Луценко повідомив, що ГПУ спільно з СБУ виявлено факт фінансування С. Курченком масових акцій протесту у містах України) In https://www.gp.gov.ua/ua/news.html?_m=publications&_t=rec&id=220231&fp=60.

Daniels Laura. "How Russia hacked the French election". POLITICO, 23.04.2017 In https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

Ellen Nakashima. "Inside a Russian disinformation campaign in Ukraine in 2014". The Washington Post, 25.12.2017 In https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html?utm_term=.f64454e2ed36.

European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)).

Grassegger Hannes and Krogerus Mikael. "Fake news and botnets: how Russia weaponised the web". The Guardian, 02.12.2017 In https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia

Horbulin Volodymyr and others. 2017. The World Hybrid War: Ukrainian Forefront: monograph, Kyiv: The National Institute for Strategic Studies, in Ukrainian. (Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017, с. 496).

Horbulin Volodymyr. 2017. "Active measures" of the USSR against USA: preface to hybrid war: analytical report. Kyiv: The National Institute for Strategic Studies.

International Criminal Court. The Office of the Prosecutor. Report on Preliminary Examination Activities (2016). Official website. In https://www.icc-cpi.int/iccdocs/otp/161114-otp-rep-PE_ENG.pdf.

Jong de Sijbren, Sweijs Tim, Kertysova Katarina, Bos Roel. 2017. Inside The Kremlin House Of Mirrors. How Liberal Democracies can Counter Russian Disinformation and Societal Interference. The Hague Centre for Strategic Studies.

Leonnig Carol D., Hamburger Tom and Helderman Rosalind S.. "Russian firm tied to pro-Kremlin propaganda advertised on Facebook during election". The Washington Post, 06.09.2017 In https://www.washingtonpost.com/politics/facebook-says-it-sold-political-ads-to-russian-company-during-2016-election/2017/09/06/32f01fd2-931e-11e7-89fa-bb822a46da5b_story.html?utm_term=.de6206fe1b8e.

Nimmo Ben. "How A Russian Troll Fooled America". Atlantic Council's Digital Forensic Research Lab, 14.11.2017 In https://medium.com/dfrlab/how-a-russian-troll-fooled-america-80452a4806d1.

Sanovich Sergei. 2017. Computational Propaganda in Russia: The Origins of Digital Misinformation. University of Oxford.

Weedon Jen, William Nuland and Stamos Alex. 2017. Information Operations and Facebook. Facebook Inc.