FOLIA 328

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 11(1) (2021)
ISSN 2657-8549
DOI 10.24917/26578549.11.1.1

Andrzej Jacuch
ORCID ID: 0000-0003-1013-6107

Military University of Technology, Warsaw

Disinformation and Propaganda Target Europe – Russia's Disinformation Activities against Ukraine

Introduction

The use of hybrid tactics and means to illegally annex[1] Crimea and destabilize Ukraine has changed our perception of the world's security. The Russian Federation (RF) takes advantage of the geographical proximity of neighboring countries and their existing social relations and economic ties for actions targeted at the security of these countries. These threats, including disinformation and propaganda, are growing along with today's more advanced level of interconnectedness, facilitated through the Internet and social media. The RF has used cyberattacks, fake news, and propaganda to achieve its strategic foreign policy objectives. These activities have intensified during the COVID-19 pandemic. The consequences of the pandemic will be far-reaching. Countries will have to adapt their military and civil capabilities to traditional security threats as well as to new challenges resulting from, *inter alia*, technological developments, climate change, pandemics, and mass migration. A dramatic change in the perception of threats is likely to be one of the consequences of the current pandemic. Strategic communication, which must directly reach, inform, and guide populations, has become a critical aspect.

The aim of this paper is to substantiate the thesis that the Russian Federation has been extensively using disinformation and propaganda against Ukraine and that informational resilience is the key to countering such actions. Qualitative research methods were used in the research process, including analysis based on interviews with experts, public records, policy documents, legislative acts, and media statements, as well as work experience, synthesis, abstracting, comparison, generalization, and implication.

[1] The EU uses the term of "illegal annexation of Crimea".

This article consists of four sections. The first offers an assessment of hybrid threats, with a focus on disinformation. The next section considers the Russian concept of information warfare. The third examines the RF information operations against Ukraine. The fourth presents how the EU and its members counter disinformation. The closing remarks reiterate that "informational resilience" is the appropriate and necessary strategic response to disinformation and propaganda.

Hybrid Threats – Disinformation

Hybrid concepts and strategies target vulnerabilities – from disinformation and propaganda to cyber-attacks on critical information systems, through the disruption of critical services and infrastructures to undermining public trust in government institutions or social cohesion. The diversity of hybrid tactics masks the thorough planning behind the spectrum of tools used and the effects they produce[2].

Hybrid conflict-specific phenomena are not only difficult to classify but are differently interpreted by countries and security organizations, which significantly complicates creating a cohesive approach to fighting hybrid threats. The growing use of hybrid tactics and methods within an increasing number of conflict areas raises questions about how to adjust or even change national defense strategies to face the new challenges of the 21st century. It will not be possible to categorize many future conflicts as solely conventional or irregular, state or non-state.

For several years in contemporary science publications, the problem of the asymmetry and hybridity of modern conflicts has increasingly been addressed. Hybrid conflict, as a specific combination of conventional and irregular operations, has been known for centuries. However, the term "hybrid" that became relevant after Russia's illegal annexation of Crimea and its continued aggression in Eastern Ukraine became essential in conceptualizing modern warfare and threats[3].

Hybrid threats combine military and non-military, covert and overt means, including disinformation, cyberattacks, economic pressure, deployment of irregular armed groups, and use of regular forces. Hybrid methods are used to blur the lines between war and peace and to sow doubt in the minds of target populations[4].

The EU explains that hybrid threats combine conventional and unconventional military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives. Hybrid campaigns are multidimensional, combining coercive and subversive measures and using both conventional and unconventional tools and tactics. They are designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create

[2] R.D. Thiele, *Building Resilience Readiness against Hybrid Threats – A Cooperative European Union / NATO Perspective*, "Focus on Defence and International Security" 2016, No. 449, p. 2.

[3] E. Bajarūnas, V. Keršanskas, *Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome*, "Lithuanian Annual Strategic Review" 2018, Vol. 16, p. 123.

[4] *NATO's Response to Hybrid Threats*, *What are the Hybrid Threats NATO Faces?,* NATO Website, 2021.

confusion to hinder swift and effective decision-making. Hybrid threats can range from cyberattacks on critical information systems to the disruption of critical services, such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social divisions[5].

Information operations and warfare in cyberspace are particularly challenging threats[6]. Psychological character is an important feature of hybrid conflicts, as is using cyberspace to destroy an opponent's information systems and spread propaganda content and fake news. The most well-known example of this form of warfare is Russia's approach to Ukraine, which has involved a combination of the above-mentioned activities.

The second example of hybrid threats is ISIS activities in the Middle East. There have been two hybrid warfare models. In Syria and Iraq, hybrid activities have been carried out by a terrorist organization – a non-state entity. In the case of the Ukrainian conflict, actions are covered by the state[7]. Batorowska et al. (2019)[8] discuss strong manipulative information activities conducted by the RF and ISIS.

Events in Ukraine made the international community aware that a hybrid war can be a way of deliberately reducing the scale of military operations in order to make it impossible to clearly indicate the aggressor and declare a state of war, in effect avoiding the reaction of social communities. Ambiguity is used to complicate and undermine the decision-making processes of the opponent. The situation is tailored to make a military response politically irrational and a political response difficult. Today, hybrid threats constitute a greater risk to national or international security than conventional methods of warfare. Hybrid warfare can be an effective method of achieving intended goals. Because of hybrid threats – leading to a hybrid war – global powers are redefining their security policy and implementing new strategies.

RF Informational Influence

Traditional media are increasingly working with the Internet and mass media as sources of information and means of influencing the minds of citizens. Information on the Web is becoming accessible worldwide, quickly distributed, and socially significant. The purpose of information activities is to control the process of changing people's consciousness – their worldview, attitude to society, and impression of the state. The danger for people is the loss of their own will and, for the state, its sovereignty. The main goals of information activities are political disorientation of the

[5] *Common Action to Counter Hybrid Threats*, EU2019FI, Finland's Presidency of the Council of the European Union, 2019.

[6] A. Jacuch, *Countering Hybrid Threats: Resilience in the EU and NATO's Strategies*, "The Copernicus Journal of Political Studies" 2020, No. 1, pp. 5–26.

[7] Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, "Przegląd Bezpieczeństwa Wewnętrznego. Wojna Hybrydowa – Wydanie Specjalne" 2015, p. 45.

[8] H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019.

opponent, disinformation about their own resources, actions aimed at defeating or blocking data channels for the purpose of disorientation and disorganization, creating an atmosphere of tension, and influencing the mass consciousness in order to demoralize and spread panic. The constant increase in information flows makes them very difficult to control. Hence, the main task during a confrontation in the information sphere is not to control the flow of information but to control the algorithm of information movement, which will allow it to be decrypted, thus protecting society and its governing institutions[9].

The RF and China have the greatest monitoring and information offensive capabilities[10]. However, each of these countries has developed its own methodology and objectives. In Russia, the importance of information weapons was already highlighted under President Boris Yeltsin when official state documents declared that after nuclear weapons, information weapons would play a major role in future conflicts. A general war with Europe remains an unlikely scenario. The RF has lower economic and conventional military capabilities compared to the West. Hence, it attaches the greatest importance to both nuclear deterrence and asymmetric methods and instruments, i.e., means of maintaining strategic parity with the West. Dmitri Trenin says that "since February 2014 the FR has been operating in a de facto war mode, and the leader of the war is the President of the RF"[11].

The Russian war doctrine recognizes the information struggle as a key element of modern military action, and Russia has been developing capabilities in this area[12]. In 2013, the Chief of General Staff of the Russian Armed Forces, General Valerij V. Gerasymov, wrote: "The role of non-military means of achieving political and strategic objectives has increased and in many cases exceeded military capabilities in its effectiveness"[13]. According to Gerasymov's doctrine, non-military methods of conducting conflict – including information warfare – are more effective than conventional weapons. Russian strategists have developed an approach – "information confrontation"[14] – where it is possible to distribute Russian propaganda during both war and peace, reflecting its "permanent" character. Russian military

[9] J. Donovan, P.M. Krafft, *Disinformation by Design: The Use of Evidence Collages and Platform Filtering in a Media Manipulation Campaign*, "Political Communication" 2020, Vol. 37, No. 2, pp. 199–206.

[10] N. Beauchamp-Mustafaga et al., *Hostile Social Manipulation: Present Realities and Emerging Trends*, RAND Corporation, Santa Monica 2019.

[11] D. Trenin, *Demands on Russian Foreign Policy and its Drivers: Looking Out Five Years*, Carnegie Moscow Center 2017.

[12] J. Darczewska, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle Doktryny Wojennej Rosji*, "Punkt Widzenia" 2015, No. 50, p. 14.

[13] В.В. Герасимов, *Ценность науки в предвидении, Новые вызовы требуют переосмыслить формы и способы ведения боевых действий*, "Военно-промышленный курьер" 2013, No. 8 (476).

[14] Г.М. Шушков, И.В. Сергеев, *Концептуальные основы информационной безопасности Российской Федерации* [in:] *Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сборник научных трудов III, Всероссийской заочной*

literature outlines two types of information warfare: 1) consistently conducted information-psychological warfare targeting the armed forces and the population of an adversary, and 2) information technology warfare on adversary technical systems conducted during conflicts by Russian special forces[15].

Gerasymov states that in the 21st century, there will be a tendency to blur the borders between the states of war and peace. Wars will not be preceded by formal notice. It is becoming more important to use a variety of political, economic, and non-military instruments, manipulating the moods of people living in the conflict area. These activities are supported by military measures, especially those of information warfare and special unit operations. During hybrid operations, information operations are widely used, allowing the user to eliminate the enemy's advantage in armed conflict. These include the use of internal opposition to create a permanent front across the entire territory of an opponent, information impact, and constantly changing forms and modes of influence. For Gerasymov, an important element is also blurring the lines between levels of action – strategic, operational, and tactical – and between offensive and defensive operations[16].

From the Russian point of view, information warfare is not an activity limited to periods of officially declared war or even to the initial phase of the conflict preceding the start of the warfare. Instead, it is a continuous activity, regardless of the state of relations with the adversary. Unlike other forms and methods of conflict, informational confrontation is carried out continuously, even during peacetime[17].

Russia's information activities are based on a narrative in which "the world is threatened on the one hand by religious and political radicalism (Islamists, fascists, nationalists) and on the other hand by Western postmodern liberalism, behind which lies the American aspirations for global hegemony. In this narrative Russia is presented as the main defender of a stable international order, traditional state sovereignty and civilisational and political pluralism in the world"[18]. Russia uses its information tools to advance its foreign policy goals. They have developed its capabilities in three main areas: 1) internally and externally focused media with a substantial online presence; 2) use of social media and online discussion boards and comment pages as a force multiplier to ensure Russian narratives achieve broad reach and penetration; and 3) language skills, in order to engage with target audiences on a wide front in their own language[19].

научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва), Е.А. Певцовой (ed.), Moscow State Regional University, Moscow 2016, pp. 1–6.

[15] N. Beauchamp-Mustafaga et al., *Hostile Social Manipulation…*, op. cit., p. 57.

[16] В.В. Герасимов, *Ценность науки в предвидении…*, op. cit.

[17] N. Beauchamp-Mustafaga et al., *Hostile Social Manipulation…*, op. cit., pp. 30–57.

[18] W. Rodkiewicz, J. Rogoża, *Potiomkinowski konserwatyzm, ideologiczne narzędzie Kremla*, "Punkt Widzenia" 2015, No. 48, p. 19.

[19] K. Giles, *Russia's Toolkit, The Russian Challenge*, Chatham House Report, Royal Institute of International Affairs, London 2015, p. 47.

The official anti-Western channels are the RT (formerly Russia Today TV) and the Sputnik news portal. The strategy of the RF's information activities is to throw a lot of often very abstract information into the information space – a "smokescreen" for a real disinformation purpose. The stream of information is released into the media space for a specific purpose – to hide the real disinformation by means of a simple psychological mechanism. Within the stream of abstract and seemingly false information, the recipient will be able to accept as true the one that seems most logical and true. This is the assumed goal of the disinformation campaign[20].

The official Russian quasi-media project – Sputnik's website – has a disinformation impact together with many entities that directly or indirectly serve the interests of the RF. The information prepared and disseminated by Sputnik is transmitted to varying degrees through other portals that can be described as "satellites". Through these networks, this information reaches a wider audience. These portals publish factual content but change its meaning and add a negative narrative to it, which contradicts journalistic integrity. Sometimes these portals create news based on subjective opinions or untested sources. Often, by using simple and non-journalistic language and through populist slogans, they gain the support of more radical and shocking content-oriented audiences[21].

Intentional disinformation and propaganda are spread both in standard media and in cyberspace. The aim of the Russian information war is to subjugate the elites and societies of other countries unnoticeably by using various secret and open channels (secret, diplomatic, and media services), psychological influence, and ideological and political diversion. The RF uses all possible information channels – traditional media, think-thanks, social networks, websites, etc.

Ukraine – The Information Threat's Impact

The leading component of hybrid is information warfare. The constant development of mass communication systems creates broad opportunities to manipulate the consciousness of the population of an adversary with other ideas. The hybrid war in Ukraine is not a new and unknown type of conflict, but it is different from previous conflicts in many respects. Propaganda and disinformation, cyber-attacks, the subsequent low morale of Ukrainian forces, and lack of military mobility were the main reasons that Crimea was handed over to Russia without the so-called "single shot"[22].

In the summer of 2013, in Vradiivka[23], there were protests that turned into a civil society expedition to Kiev and ignited Euromaidan protests. The reasons for

[20] S. Gliwa, A.K. Olech, *Relacje polsko-czeskie a rosyjska dezinformacja. Czy destabilizacja stosunków jest możliwa?*, "CyberDefence24.pl" 2020.

[21] Ibidem.

[22] A. Jacuch, *Countering Hybrid Threats…*, op. cit., pp. 5–26.

[23] In June 2013, a rape of a local resident by policemen caused riots in Vradiivka and nationwide. Since then, Vradiivka has become a symbol for protests against police crimes and the arbitrariness of the justice system.

the protests were the lack of contact between the Ukrainian leadership and civil society, the poor socio-economic situation, the aspirations of oligarchical groups, and the desire for integration with the European Union.

In February 2014, the RF illegally annexed Crimea and Sevastopol. The next stage was an attempt to destabilize the eastern and southern regions of Ukraine in order to create the so-called "Novorossiya". In 2014, the RF was not seen as a potential threat. Ukraine was prepared to take both defensive and offensive action in a Western direction. Russia took advantage of Ukraine's weakness to safeguard the freedom of military action in the Black Sea and the Azov Sea, to prevent Ukraine's integration into the EU and NATO, to initiate reviews of the borders and norms of international law that have been in place since the end of the Second World War, and, as a result, to bring about a new division of spheres of influence.

The illegal annexation of Crimea and the Donbas operations were carried out by the RF through the use of hybrid forms and methods of warfare, including a propaganda campaign, a diplomatic blockade of legal mechanisms of international organizations, and economic pressure with the use of the energy factor. Propaganda and disinformation have played a key role in RF activities. Russian propaganda has created an ideological platform for the "Russian World" to influence the awareness of Ukrainian society.

The RF is influencing the unity of the European Community, seeking to strengthen its influence and control over processes on the European continent in order to establish a new order in Europe according to the RF scenario. Its objectives are to prevent the countries that emerged in the former USSR – Georgia, Moldova, and Ukraine – from joining the EU and NATO; to break the Euro-Atlantic and European unity; to make European countries dependent on the RF; and to seek a division into spheres of influence of a "Yalta-2.0" type. In order to achieve these objectives, the RF is using intelligence activities, discrediting state structures, supporting populist movements, and the mass media, which spread anti-NATO, anti-European, and anti-American sentiments in the societies of EU countries and continue supporting the "compatriots'" and sympathizers' environment.

Through disinformation, fake news, and information-gathering, denying or distorting facts, it is possible to manipulate people, convince politicians, disinform society, and shape its collective consciousness, thus creating an alternative perception of reality, an alternative social consciousness. Russia has many years of experience in conducting the information struggle and using propaganda methods which, together with an extensive campaign on the Internet and social media, is conducted in Ukraine. Their basic instrument remains specpropaganda: contemporary Russian information battles clearly refer to those of the Cold War era[24]. They include: 1) the principle of mass and long-term action – e.g., the propaganda stereotype of the "orange plague" and "bandits" that has been repeated since 2003; 2) the principle

[24] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, "Punkt Widzenia" 2014, No. 42, p. 25.

of desired information – for example, Russians and the Russian-speaking population expect to defend their rights; 3) the principle of emotional arousal – a message to arouse emotion; 4) the principle of comprehensibility – a simplified message in black and white; 5) the principle of supposed obviousness – evoking association of the propaganda thesis with the created political myths: bandits – fascism, Majdan – chaos, etc.[25]

To promote content favorable to the information war, the RF has used messages from President Putin and high-ranking Russian officials and soldiers, as well as the so-called "troll armies" paid for by the authorities, whose task is to comment on media reports in accordance with pro-Russian and anti-Western rhetoric. The activity of the "trolls" is particularly visible on the Internet, especially social networking sites and discussion forums, as well as on news sites. As part of the information struggle, Russia is setting up anti-Western websites where most of the information is presented in a pro-Russian way, and some of it is false[26]. The Russian authorities also use information warfare units, which were established in 2017[27].

Information and informational and psychological operations are designed to transform the image of the world that exists in the consciousness of the opponent into the image desired by the propagator. This can be done through techniques of camouflaging the source. Often, the goal is achieved by creating an artificial enemy or by identifying substitute targets that conceal the sender's essential intentions. There is a whole set of manipulative techniques used in crisis situations[28]. The authors of the propaganda message, in this type of operation, base them on the emotions of the recipients. The strength of disinformation built in this way is that it refers to phenomena and fears familiar to the recipient and thus seems credible to him, exaggerating one aspect of the matter and diminishing another[29].

Russia's information operations in Ukraine were crucial to the successful seizure of Crimea and operational expansion into the Donbas region. This effort can be broken down into the following three groups: 1) Russia's preceding "humanitarian" foreign policy, 2) pro-Russian media within Ukraine, and 3) global pro-Russian media aimed at the West[30]. Russia won the media war with Ukraine. A divided Ukraine, which was experiencing a political crisis, was unable to effectively oppose the RF.

---

[25] Ibidem.

[26] F. Bryjka, *Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej* [in:] *Bezpieczeństwo personalne a bezpieczeństwo strukturalne III. Czynniki antropologiczne i społeczne bezpieczeństwa personalnego*, T. Grabińska, Z. Kuźniar (eds.), WSO WL, Wrocław 2015, p. 127.

[27] *Rosja: Siergiej Szojgu o istnieniu oddziału żołnierzy wojny informacyjnej*, ONET Wiadomości, 2017.

[28] P. Polko, R. Polko, *Bezpiecznie już było. Jak żyć w świecie sieci, terrorystów i ciągłej niepewności*, Helion, Gliwice 2018, p. 97.

[29] Ibidem.

[30] B. Perry, *Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations*, "Small Wars Journal" 2015.

Consistency in taking advantage of the disinformation and propaganda and the large number of Russians in eastern Ukraine led to an unclear situation and helped to destabilize the region. The experience gained in influencing Ukraine's population through misinformation may serve to achieve further geostrategic goals in other countries, in particular, Poland, the Baltic States, and other Central and Eastern European countries.

The EU Countering Disinformation

The EU defines "disinformation" as verifiably false or misleading information that is created, presented, and disseminated for economic gain or to intentionally deceive the public – it distorts public debate, undermines citizens' trust in institutions and media, and even destabilizes democratic processes, such as elections[31].

Since 2015, the EU has been implementing measures to address disinformation and to protect its democratic systems and public debates. To address Russia's disinformation campaigns, the EU set up the East StratCom Task Force in March 2015[32]. It develops communication products and campaigns focused on explaining the EU. It also reports on and analyses disinformation trends, explains and corrects disinformation narratives, and raises awareness of disinformation. To raise awareness of disinformation, it produces the weekly Disinformation Review (EUvsDisinformation – webpage). In 2016, the EU adopted a joint framework to counter hybrid threats and foster resilience[33].

In response to hybrid activities by state and non-state actors, in June 2018, the EU identified areas where action should be intensified in order to further deepen and strengthen its response to these threats, including, among others, such areas as strategic communications and situational awareness[34]. A package of measures to support free and fair European elections included protection against cybersecurity incidents and fighting disinformation campaigns. The EU's action plan against disinformation addressed potential threats to the elections and strengthening the resilience of the EU's democratic systems[35]. A Rapid Alert System on Disinformation (RAS) was set up to facilitate the sharing of insights related to disinformation campaigns and to coordinate responses. The EU member states and the ENISA carried

[31] *Countering Disinformation*, EEAS, 2019.

[32] *Questions and Answers about the East StratCom Task Force*, EEAS, 2018.

[33] *Joint Framework on Countering Hybrid Threats – A European Union Response*, JOIN(2016) 18 final, Joint Communication to the European Parliament and the Council, Brussels 2016.

[34] *Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*, JOIN(2018) 16 final, Joint Communication to the European Parliament, the European Council and the Council, Brussels 2018.

[35] *Action Plan against Disinformation*, JOIN(2018) 36 final, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions, Brussels 2018.

out a live test of their preparedness, and a progress report on the fight against disinformation was published[36].

Conclusions

To respond to hybrid threats in today's global interconnected world, with its new technologies, the Internet, social media, and artificial intelligence, we have to develop comprehensive security by not only developing military capacity but especially by enhancing civil preparedness in critical areas, enabling monitoring, mitigation, recovery from, and countering potential hybrid attacks. A shift from the classic military confrontation to information warfare can be seen in recent years. In fact, societies are more connected not only technologically but in practically all spheres of life. In the information era, globalization and the Internet have brought new capabilities as well as new vulnerabilities.

The RF is trying to change the global order to a multipolar system in which the RF is one of the main actors. This is particularly visible in Central and Eastern Europe. In the current geostrategic situation, Russia influences European countries by non-military means, mainly through the actions of intelligence, disinformation, and propaganda, and also economically (oil and gas). Russia's theory of information war relates to a wide range of activities of a social, political, military, economic, intelligence, counterintelligence, propaganda, diplomatic, psychological, IT, and educational nature[37].

Unlike conventional war, the focus in Ukraine was on non-military activities, the use of propaganda and disinformation, cyber-attacks, provoking unrest on political grounds, destabilizing the economy, applying financial pressure, spreading corruption and crime, conflicting ethnic groups, illegal border crossings and disinformation about their purpose, attacks on electricity networks and power plants, etc. The course of the conflict also shows that the Russians' aim has not been to occupy Ukraine but to destabilize its eastern region[38].

Moscow's media campaign against Ukraine was surprisingly effective – not only in Russia itself but also among Western public opinion. The practice of the Russian Information War combines proven tools with modern technology and capabilities. Some of these tools are recognized as elements of the subversive campaign of the Cold War[39]. The main lesson identified from the conflict in Ukraine is that if territorial

[36] *Report on the Implementation of the Action Plan against Disinformation*, JOIN(2019) 12 final, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Region, Brussels 2019.

[37] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej*..., op. cit., p. 10.

[38] A. Jacuch, *Civil Preparedness – Military Mobility* [in:] *Security and Russian Threats*, M. Banasik, P. Gawliczek, A. Rogozińska (eds.), Jan Kochanowski University of Kielce, Kielce 2019, pp. 231–248.

[39] H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu*..., op. cit., pp. 206–207.

integrity is under any form of hybrid aggression, under an information campaign, to resist effectively, adequate counter-means have to be developed and deployed at national and regional levels, including such measures as counter-aggression in information and cyberspaces.

The Baltics, the Visegrád Group, and Balkans countries are particularly exposed to hybrid threats. This is because of Russia's political objectives, geographical proximity, economic influence, Russian-speaking minorities and/or economic migrants, and possibly cultural codes affected by Soviet dominance in these regions during the Cold War[40]. In today's globally interconnected world, information operations are regularly used by aggressive and malicious states and non-state actors. Strategic communication and adaptive informational resilience are of fundamental importance – identifying, monitoring, and countering disinformation and fake news, will allow countries to resist and recover from any kind of information operations of potential opponents.

References

Action Plan against Disinformation, JOIN(2018) 36 final, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions, Brussels 2018.

Bajarūnas E., Keršanskas V., *Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome*, "Lithuanian Annual Strategic Review" 2018, Vol. 16.

Batorowska H., Klepka R., Wasiuta O., *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019.

Beauchamp-Mustafaga N., Casey A., Demus A., Harold S.W., Matthews L.J., Mazarr M.J., Sladden J., *Hostile Social Manipulation: Present Realities and Emerging Trends*, RAND Corporation, Santa Monica 2019.

Bryjka F., *Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej* [in:] *Bezpieczeństwo personalne a bezpieczeństwo strukturalne III. Czynniki antropologiczne i społeczne bezpieczeństwa personalnego*, T. Grabińska, Z. Kuźniar (eds.), WSO WL, Wrocław 2015.

Common Action to Counter Hybrid Threats, EU2019FI, Finland's Presidency of the Council of the European Union, 2019.

Countering Disinformation, EEAS, 2019.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, "Punkt Widzenia" 2014, No. 42.

Darczewska J., *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle Doktryny Wojennej Rosji*, "Punkt Widzenia" 2015, No. 50.

Donovan J., Krafft P.M., *Disinformation by Design: The Use of Evidence Collages and Platform Filtering in a Media Manipulation Campaign*, "Political Communication" 2020, Vol. 37, No. 2.

Giles K., *Russia's Toolkit, The Russian Challenge*, Chatham House Report, Royal Institute of International Affairs, London 2015.

[40] A. Jacuch, *Countering Hybrid Threats…*, op. cit., pp. 5–26.

Gliwa S., Olech A.K., *Relacje polsko-czeskie a rosyjska dezinformacja. Czy destabilizacja stosunków jest możliwa?*, "CyberDefence24.pl" 2020.

Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats, JOIN(2018) 16 final, Joint Communication to the European Parliament, the European Council and the Council, Brussels 2018.

Jacuch A., *Civil Preparedness – Military Mobility* [in:] *Security and Russian Threats*, M. Banasik, P. Gawliczek, A. Rogozińska (eds.), Jan Kochanowski University of Kielce, Kielce 2019.

Jacuch A., *Countering Hybrid Threats: Resilience in the EU and NATO's Strategies*, "The Copernicus Journal of Political Studies" 2020, No. 1.

Joint Framework on Countering Hybrid Threats – A European Union Response, JOIN(2016) 18 final, Joint Communication to the European Parliament and the Council, Brussels 2016.

NATO's Response to Hybrid Threats, *What are the Hybrid Threats NATO Faces?,* NATO Website, 2021.

Perry B., *Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations*, "Small Wars Journal" 2015.

Polko P., Polko R., *Bezpiecznie już było. Jak żyć w świecie sieci, terrorystów i ciągłej niepewności*, Helion, Gliwice 2018.

Questions and Answers about the East StratCom Task Force, EEAS, 2018.

Report on the Implementation of the Action Plan Against Disinformation, JOIN(2019) 12 final, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Region, Brussels 2019.

Rodkiewicz W., Rogoża J., *Potiomkinowski konserwatyzm, ideologiczne narzędzie Kremla*, "Punkt Widzenia" 2015, No. 48.

Rosja: Siergiej Szojgu o istnieniu oddziału żołnierzy wojny informacyjnej, ONET Wiadomości, 2017.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego. Wojna Hybrydowa – Wydanie Specjalne" 2015.

Thiele R.D., *Building Resilience Readiness against Hybrid Threats – A Cooperative European Union / NATO Perspective*, "Focus on Defence and International Security" 2016, No. 449.

Trenin D., *Demands on Russian Foreign Policy and its Drivers: Looking Out Five Years*, Carnegie Moscow Center 2017.

Герасимов В.В., *Ценность науки в предвидении, Новые вызовы требуют переосмыслить формы и способы ведения боевых действий*, "Военно-промышленный курьер" 2013, No. 8 (476).

Шушков Г.М., Сергеев И.В., *Концептуальные основы информационной безопасности Российской Федерации* [in:] *Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сборник научных трудов III, Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва)*, Е.А. Певцовой (ed.), Moscow State Regional University, Moscow 2016.

Disinformation and Propaganda Target Europe – Russia's Disinformation Activities against Ukraine

Abstract

Disinformation and propaganda or information warfare have been employed by the Russian Federation (RF) to obtain a strategic advantage in Ukraine as well as in other geopolitically important countries. The impact of information warfare has been amplified with the COVID-19 pandemic. Disinformation targets Western countries, particularly through the Internet and social media. Russian war doctrines recognize information warfare as a key element of modern military action, and the RF develops capabilities in this area. This paper aims to identify, analyze, and assess the Russian actions against Ukraine in the Crimea and Donbas regions, and particularly the conduct of information warfare by the RF. The fusion of disinformation, propaganda, and other covert powers can be a coercive tool to be used in conflicts. The main hypothesis stipulates that hybrid threats, particularly information warfare, have been tested by the RF in Ukraine to evaluate its concepts, methods, and effectiveness in preparation to conduct aggressive actions in other countries. Coordinated responses to disinformation and propaganda, particularly informational resilience, should be bolstered.

Słowa kluczowe: UE, Ukraina, zagrożenia hybrydowe, dezinformacja, wojna informacyjna, odporność

Key words: EU, Ukraine, hybrid threats, disinformation, information warfare, resilience

Andrzej Jacuch

Dr. Eng., academic at the Institute of Security and Defence at the Military University of Technology in Warsaw. He is a former Polish Navy Captain who was employed as a civilian at NATO's International Staff. Before NATO, he worked at the Ministry of Transport and the Naval Academy, Gdynia. E-mail: andrzej.jacuch@wat.edu.pl