OPEN Publications
ISSN 2957-7160 (Online)
ISSN 2957-7799 (Print)

INFORMATION AS AN INSTRUMENT OF POWER

LESSONS LEARNED FROM THE WAR IN UKRAINE

Volume 7 | Number 6 | Fall 2022

OPEN Publications (2022)

“Information as an instrument of power - Lessons learned from the war in Ukraine”

Contributing Author	Dr. Andrew N. Liaropoulos
OPEN Capability Leader	Col Geert Marien
OPEN Managing Editor	Mr Oke Thorngren
OPEN Operations Manager	Col Georgios Kotas
Action Officer	Col Georgios Kotas
OPEN Editorial Review Board	Cdr Silvio Amizic Cdr Alban Morel LtC Stig Frankrig LtC Christopher Soemod Cdr Jeff Gulliver LtC Alfredo Marroccelli Maj Mithat Almaz Mr Ian Birdwell Ms Rachel Grimes Mr Neil Schuehle

About the author:

Dr. Andrew N. Liaropoulos is Assistant Professor in University of Piraeus, Department of International and European Studies, Greece. He earned his master’s degree in Intelligence and Strategic Studies at Aberystwyth University and his Doctorate Diploma at Swansea University. His research interests include international security, intelligence reform, strategy, European security, foreign policy analysis, cybersecurity and information warfare. Dr. Liaropoulos is also a senior analyst in the Research Institute for European and American Studies (RIEAS) and a member of the editorial board of the Journal of Information Warfare (JIW).

Let us know your thoughts on

“Information as an instrument of power - Lessons learned from the war in Ukraine”

by emailing us at:

editor@openpublications.org

Disclaimer

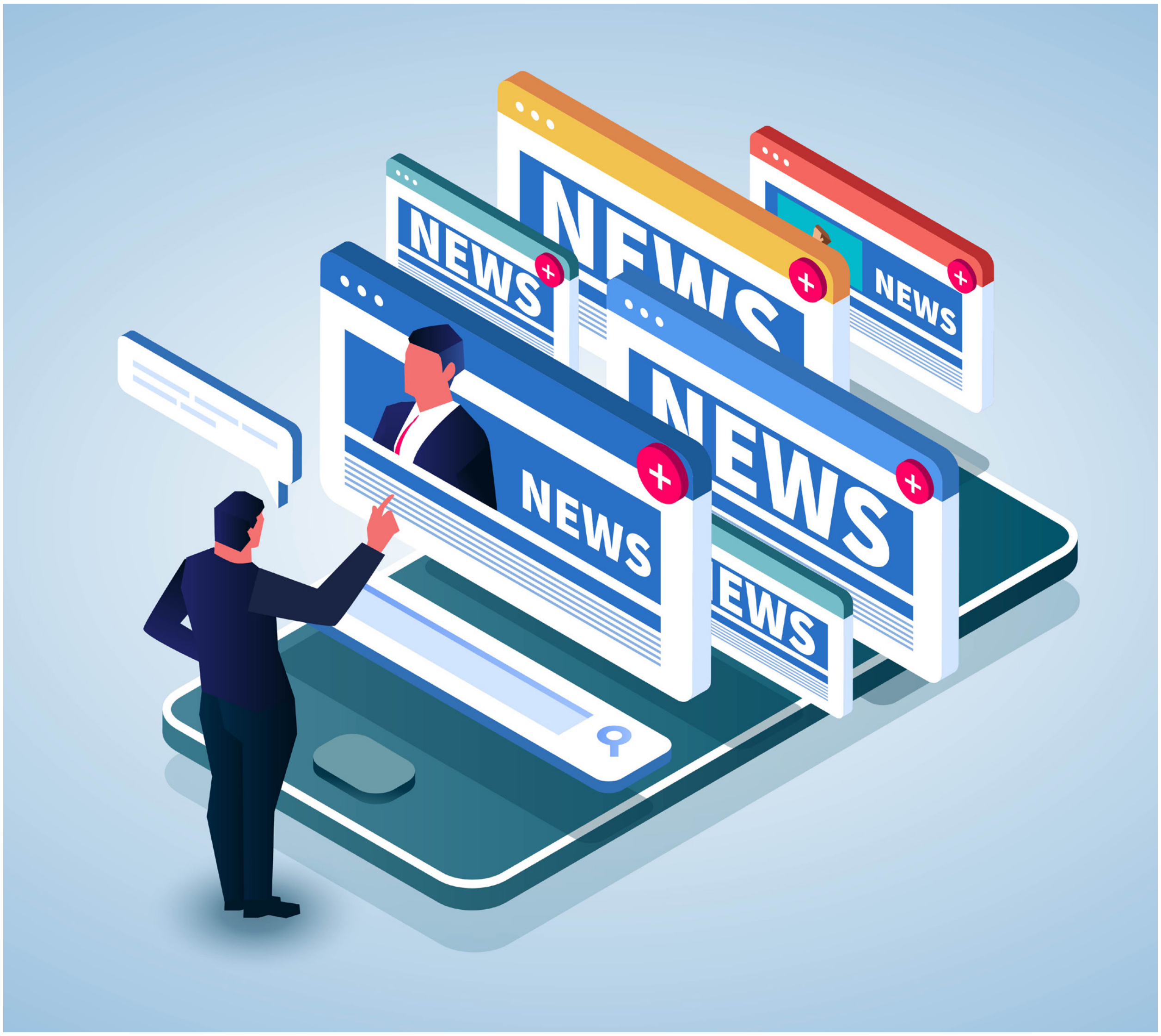
OPEN publications are produced by Allied Command Transformation/Strategic Plans and Policy; however OPEN publications are not formal NATO documents and do not represent the official opinions or positions of NATO or individual nations. OPEN is an information and knowledge management network, focused on improving the understanding of complex issues, facilitating information sharing and enhancing situational awareness. OPEN products are based upon and link to open-source information from a wide variety of organisations, research centres and media sources. However, OPEN does not endorse and cannot guarantee the accuracy or objectivity of these sources. The intellectual property rights reside with NATO and absent specific permission OPEN publications cannot be sold or reproduced for commercial purposes. Neither NATO or any NATO command, organization, or agency, nor any person acting on their behalf may be held responsible for the use, which may be made of the information contained therein.

Information as an instrument of power - Lessons learned from the war in Ukraine

Table of Contents

Executive Summary

Information is an essential element of state power used throughout history in order to exert influence on other actors and achieve certain political objectives. This paper reviews the way Russia has ‘weaponized’ information in the cases of the Crimea’s annexation in 2014 and the ongoing, since February 2022, war in Ukraine. The evidence from the above case studies reveal the various means and methods that Russia has employed. The Kremlin, via its information apparatus has exploited the Internet and social media platforms, in order to spread disinformation, construct strategic narratives and influence the decision-making processes of targeted audiences (mainly Ukraine and NATO member-states). Though the direct results of such operations are hard to measure, there is evidence that they have had effect in both operational and strategic terms. Confronting this challenge requires a number of measures that range from the construction of counter narratives and the use of social media algorithms to detect fake news, to the internet literacy of the population and the projection of objective reporting to Russian-speaking audiences.



1. Introduction

Information is an instrument of power used as a weapon since the beginning of human history. Information and communication technologies (ICTs) have turned the world into a global and highly interconnected information network. Information operations exploit emotions and beliefs and take place in the minds of human beings. States use information operations in an attempt to shape perceptions, manage public opinion and steer the policy-making process[1]. Russia is no exception to this. Over the past years, during both peacetime and wartime, Russia has 'weaponized' information, in order to serve its political ends. Russia has conducted several multifaceted information operations that aim to undermine Ukraine - as part of the annexation of Crimea in 2014 and the ongoing, since February 2022, war - and to divide the West (NATO/EU member-states) that supports Ukraine. Russia has spread disinformation via social media platforms, deployed agents of influence, funded Western political parties and attempted to manipulate public opinion in order to influence the shaping of policy and divide the West[2].

Bearing in mind that the world is much more 'connected' nowadays than it was a few decades ago, that the target audiences of information operations are both the ruling elites and the public opinion, it is necessary to understand how Russia, an actor that aggressively utilizes information as an instrument of power, is conceptualizing information operations. Furthermore, it is critical to consider how an alliance of democracies like NATO can counter such a challenge.

2. Methodology and structure of the paper

This paper analyses information as an instrument of power. The case study used in this research is the conduct of information operations by Russia in Ukraine (both the case of the annexation of Crimea in 2014 and the ongoing Russia-Ukraine war, covering the period February-August 2022). Although the focus of the paper is on how Russia utilizes information operations and constructs narratives, short reference is also made to the Ukrainian efforts to construct counter-narratives. By comparing different paradigms, we reach safer conclusions on how to respond to this challenge. Reference to the Ukrainian efforts to construct counter-narratives is only made in relation to the second case study, that of the war that started in February 2022, since in the first case study, that of Crimea's annexation, the Ukrainian authorities were taken largely by surprise and the duration of the military operations, was rather short.

The material used, involves open source information, mainly academic reports, media outlets and raw data retrieved from online sources (mostly from websites and social media platforms). The material collected is used in order to identity the information operations' mechanisms and the strategic narratives deployed by Russia and the counter-narratives deployed by Ukraine.

[1] Leigh Armistead (ed), *Information Operations Matters. Best Practices* (Washington DC: Potomac Books, 2010).

[2] See selectively Christopher Chivvis, "Hybrid War: Russian Contemporary Political Warfare", *Bulletin of the Atomic Scientists* 73, 5 (2017): 316-321, Holger Mölder et.al. *The Russian Federation in Global Knowledge Warfare. Influence Operations in Europe and its Neighborhood* (Cham: Springer, 2021), Miriam Matthews et.al. *Understanding and defending against Russia's malign and subversive information efforts in Europe* (Santa Monica: Rand, 2021) and Lilly Bilyana, *Russian Information Warfare* (Annapolis: Naval Institute Press, 2022).

In terms of structure, the paper first offers a short theoretical discussion of the importance of information as an element of power and reviews the ways in which information has been perceived in the Russian discourse (e.g. Information Security Doctrine, Gerasimov Doctrine) and recent policy and institutional developments (e.g. RuNet). In a latter phase, the paper analyses the information campaigns attributed to Russia and the responses by Ukraine. Bearing in mind that it is nearly impossible to prove causality between certain information operations and effects observed in the information environment, the evaluation process is limited on the analysis of the strategic narratives. Since both parties blocked access to the other's social media services and internet news sites, it is rather risky to argue on the success of the information operations on certain target audiences. The papers ends with some recommendations on how to confront Russia's information operations.

3. Information as an instrument of state power

In an era characterized by the rapid development of ICTs, it is only natural that information plays a central role in any type of sociopolitical confrontation. Apart from the traditional battlefield, states have also to take into consideration the battlespace of the mind and the war of narratives. Information operations are not new, but their potential in an information-intensive environment poses a great challenge for liberal democracies. Information operations - regardless of whether they are labeled as political warfare or influence operations or exercised as an element of a broader hybrid campaign - exploit the vulnerabilities of liberal democracies and target both the elites and societies of the western states in order to influence political behavior and public opinion. The toolkit involves the dissemination of false, misleading and manipulative information in the media - especially the social media. Information operations exploit one of the most challenging characteristics of our era: ambiguity. The lines between virtual and real, domestic and international, public and private have eroded, and the result is far more ambiguity. Planting and disseminating a lie via social media is cheap and easy. On the other hand, identifying the lie, tracking its origins, and communicating 'your' truth to the same audiences is labor intensive and costly[3].

[3] Keir Giles, *The Next Phase of Russian Information Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016), 7.

3.1 Conceptualizing Russian information operations

During the past two decades, information warfare and related concepts like propaganda, strategic communication, disinformation, influence operations, subversion, reflexive control theory and, lately, hybrid warfare have been intensively debated in the Russian political discourse[4]. In general, information warfare refers to the methods and techniques used to shape political behavior. Information warfare is a tool, one among many, which is applied in order to achieve political goals. The Russian Ministry of Defence defines information warfare as the ability to undermine political, economic and social systems; carry out massive psychological campaigns against the population of a state in order to destabilize its society and government, and force a state to make decisions in the interest of its opponents. Whereas the West mainly views information operations as one of many tools when conducting a military campaign, for Russian analysts, information has a central role during both peacetime and wartime[5]. For the Kremlin, the focus in contemporary conflicts has shifted from destruction to influence; from a confrontation with weapons to a battle for people's minds. The center of gravity is the mind, and the aim is to dominate in this new battlespace, in order to reduce the necessity for conventional military power[6]. Although an old phenomenon, information operations are gaining importance due to the processes of globalization and the spread of information technologies. In the Russian case, however, two additional factors explain the centrality of this concept in shaping national policies. To begin with, Russia has a long tradition of using information operations. In the military domain, both czarist and Soviet forces were successful in the art of military deception, known as maskirovka[7]. Likewise, Soviet intelligence and security services were very keen on conducting subversion - otherwise known as political warfare or active measures[8]. Aleksandr Dugin's writings on net-centric war, Igor Panarin's analysis on information warfare, and military thinkers' input that appears in the journal Military Thought[9] are indicative of the perceptions that dominate the debate within Russia[10]. The manipulation of the information domain aims to undermine a government and influence political elites in order to trigger sociopolitical upheavals within the targeted state[11]. Russian theorists argue that information warfare is used openly by the West and in particular by the USA, to undermine Mos-

[4] See selectively Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?", *The Journal of Slavic Military Studies* 27 (2014): 101-130, Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations", *Defence Strategic Communications* 1, 1 (2015) and Ofer Fridman, "The Russian Perspective on Information Warfare: Conceptual roots and politicisation in Russian academic, political and public discourse", *Defence Strategic Communications* 2 (2017): 61-83.

[5] Ron Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare", *RUSI Journal* 160, 4 (2015): 42.

[6] Jānis Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defence Policy", *Policy Paper* 2 (Riga: National Defence Academy of Latvia, Center for Security and Strategic Research, April 2014).

[7] David Glantz, *Surprise and Maskivorka in Contemporary War* (Kansas: Fort Leavenworth, Soviet Army Studies Office, Army Combined Arms Center, 1988).

[8] Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999) and T.S. Allen and A.J. Moore, "Victory Without Casualties: Russia's Information Operations", *Parameters* 48, 1 (2018): 61-62.

[9] *Military Thought: A Russian Journal of Military Theory and Strategy* [Военная мысль] is a press organ of the Ministry of Defense of the Russian Federation. The original Russian version is published since 1918 and the English version is published since 1992. For more details see https://www.eastview.com/resources/journals/military-thought/.

[10] Thomas, "Russia's Information Warfare Strategy", 105, 117.

[11] In particular, the Russian military doctrine refers to the 'protest potential of the population'. See Rob Thornton and Marina Miron, "Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow's Strategic Thinking", *The Cyber Defence Review* 7, 3 (2022), 124-125.

cow’s exercise of sovereignty. In their eyes, Russia is a victim of information warfare. The ‘first information war’ took place during the Cold War and resulted in the demise of the Soviet Union; the ‘second information war’ took place the last decade and aimed to weaken Russia[12]. In this context, the so-called Colored Revolutions in Kyrgyzstan, Georgia and Ukraine, the Arab Spring, the 2011-12 protests in Moscow as well as the Euromaidan protests - are all examples of planned Western interventions.

Thus, another factor that should be taken into consideration when examining the way Russia approaches information operations is the level of politicization that relates to this concept. The belief that the West is waging a war that aims to disorganize governance, organize anti-government protests and influence public opinion is very common among scholars, the political elite and the public[13]. The Russian leadership supports the narrative of an information war conducted by the West against Russia. Over the past years, President Vladimir Putin and Minister of Foreign Affairs Sergey Lavrov have frequently claimed that Russia has been targeted by information operations. Public opinion surveys prove that the Russian people have embraced this narrative and are largely convinced that a western offensive against Russia has already taken place[14].

According to Van Herpen, one can identify three major strategies in the conduct of such operations: mimesis, rollback and invention. The first step involves copying public diplomacy initiatives that have been developed by the West some decades ago. Following the example of the USA and Europe, Russia established non-governmental organizations (NGOs) that are practically organized and controlled by the state. Such cases include the Russkiy Mir Foundation and the Russian International Affairs Council (RIAC). These soft tools are used to influence foreign governments and manipulate public opinion. The second strategy, rollback, is a more aggressive one and involves an attack on Western public diplomacy initiatives. This is achieved by restricting the activities of both Western and Russian NGOs that are based in Russia and are funded from abroad. The last strategy, invention, involves the hiring of lobbying firms and the establishment of think-tanks and discussion fora like the Valdai Discussion Club, which aim to improve Russia’s, image abroad[15].

Information operations are mainly conducted via the media (traditional and social media), and Russia has been very active in controlling its media sphere. The Kremlin managed to take control of domestic social media (V Kontakte), and create new media like Russia Today and Sputnik News. Media organizations like NTV, Channel One Russia and Russia 24 spread the Kremlin’s narrative not only to domestic audiences, but also to Russian-speaking viewers in other regions[16]. The Kremlin’s media strategy also aims to influence foreign public opinion. A closer look at Russian media operating abroad demonstrates their ability to influence Russian-speaking communities in Estonia, Latvia, Lithuania, Ukraine, Georgia, Moldova and even the former Soviet republics of Central Asia[17].

Russia is waging sophisticated information campaigns in order to promote its national interest. These campaigns are based on the familiar principles of political warfare and propaganda that the Kremlin conducted during the Cold War. The difference with that period is that nowadays Kremlin is not promoting a global ideology and such operations are facilitated by the ICTs and social media platforms.

[12] Margarita Jaintner, “Russian Information Warfare: Lessons from Ukraine”, in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, (Tallinn: NATO CCD COE 2015), 89.

[13] Fridman, “The Russian Perspective on Information Warfare”, 70-76.

[14] Ibid, 76-94.

[15] Marcel Van Herpen, *Putin’s Propaganda Machine: Soft Power and Russia’s Foreign Policy* (Lanham: Rowman & Littlefield, 2016).

[16] Christopher Walker, “The Authoritarian Threat. The hijacking of ‘Soft Power’”, *Journal of Democracy* 27, 1 (2016): 59-60.

[17] Thornton, “The Changing Nature of Modern Warfare”, 42.

The Russian paradigm offers a synthesis of old and contemporary methods, combining military and non-military means and fully exploiting the advantages and asymmetries of information technology[18].

Russia views cyberspace as a double-edged sword. Any information that can be found on the Internet is a potential weapon for, but also a potential threat to, Russia. The Kremlin views Internet and social media in particular, as a low-cost and highly effective tool that offers Russia an advantage, compared to the open and therefore volatile western democracies. At the same time though, there is always the fear that social media could undermine the regime[19]. The latter, considers the Internet an American product and sees the free flow of information, and therefore disinformation, as a direct threat to Russian cultural integrity and political independence. As a result, Moscow has decided to secure its borders in cyberspace and protect its national information space. After NATO recognized cyberspace as a military domain in 2016, Russia declared that RuNet, - the Russian section of the Internet - could potentially be disconnected from the global one. According to the Information Security Doctrine that was published in 2016, Russia should be able to deploy a control system that enables the Russian government to manage the Russian section of the Internet[20]. Based on the principle that an isolated network is a more secure one, the Kremlin isolated Russia from external networks in March 2022, thus operationalizing a fully state-controlled and independent network, which enables the authorities to control internet traffic and censor or suppress any information within the national information sphere. The only option for Russians to bypass this censorship is to download a virtual private network that allows them to access online information that is banned by their government[21].

The Information Security Doctrine is only the latest development in Russia's attempt to secure and nationalize its information sphere[22]. Since 2012, the Russian government has passed numerous laws that aim to control not only internet infrastructure, but also freedom of expression. In general, these laws aim to censor information, block websites that are considered a threat to the political establishment, oblige bloggers to register with the government, and require internet companies to locate servers handling Russian internet traffic inside the country and to store their users' data on these locally based servers[23].

Last, but not least, information operations are an integral part of the so-called 'new Russian way of war', encapsulated in the neologism of 'Gerasimov's doctrine'[24]. In February 2013, General Valery Gerasimov, Russia's chief of the General Staff, published a short article where he stressed the importance of non-military means in modern warfare and described a type of war waged on all fronts, with a range of actors and tools, including hackers, dissemination of fake news, as well as conventional

[18] Jolanta Darczewska, *The Devil is in the details: Information Warfare in the Light of Russia's Military Doctrine* (Warsaw: Centre for Eastern Studies, 2015), 38.

[19] Elina Treyger, Joe Cheravitch and Raphael S. Cohen, *Russian Disinformation Efforts on Social Media* (Santa Monica: Rand, 2022), 8.

[20] Justin Sherman, "Reassessing RuNet. Russian Internet isolation and implication for Russian cyber behavior", *Atlantic Council*, Issue Brief, 12 July 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/

[21] Philip Seib, "Why Russia is losing the information war in Ukraine", University of Southern Carolina, Center on Public Diplomacy, https://uscpublicdiplomacy.org/blog/why-russia-losing-information-war

22 Jaintner, "Russian Information Warfare", 88.

[23] Fridman, "The Russian Perspective on Information Warfare", 78-79 and Treyger, Cheravitch and Cohen, *Russian Disinformation Efforts on Social Media*, 148.

[24] It has been argued that there is nothing conceptually novel in the so-called Gerasimov Doctrine and the practice of warfare by Russia. The means may be different with the emergence of the ICTs, but the inherent logic of war and strategy remains the same. See Mark Galleoti, "The mythical 'Gerasimov Doctrine' and the language of threat", *Critical Studies on Security* 17, 2 (2019): 157-161.

and asymmetric military means. In the case of Crimea's annexation, many analysts identified elements of these practices in the battlefield.

3.2 Information as an instrument of power: the case of Crimea's annexation

Prior to Euromaidan, Ukraine was portrayed as the 'little brother' who depended from the older one - Russia - for support. In this narrative, Ukraine was framed as a subordinate partner that shares common origins and values with Russia. This narrative was useful for Kremlin, up to a point. It justified its involvement in the so-called near abroad, but did not justify a military operation against Ukraine. Thus, this narrative gradually changed and a new one emerged, where Ukraine was interpreted as irrational and misguided, as a traitor that has turned to the West (EU and NATO). Adding to that a more specific narrative was constructed, one that exploited fear and that was the threat of Ukrainians as Nazi, radical nationalists and right wing extremists[25].

Another strategic narrative that the Kremlin exploited portrayed Russia as a Eurasian power that had the legitimate right to control Ukraine. According to this narrative, Ukraine has been an integral part of the Russian World (Russkiy Mir) since the birth of the Russian Empire, and control over Crimea serves Russia's national interest. The notion that Russia should exert some form of control over the

[25] Irina Khaldarova, "Brother or 'Other'? Transformation of strategic narratives in Russian television news during the Ukrainian crisis", *Media, War & Conflict* 14 no.1 (2021): 3-20.

post-Soviet space is widely supported in many official documents (e.g. Russian Military Doctrine, Foreign Policy Concept)[26].

Apart from the above, Russia also exploited the deficiencies of the West and Ukraine, and urged the empowerment of nationalist and xenophobic trends that often occur in a crisis-prone Ukraine that is divided between its pro-Russian population (Russophones), living mostly in the Eastern and Southern parts of Ukraine (depicted as Novorossiya), and pro-Ukrainians (Ukrainophones), who have their stronghold in Western Ukraine[27].

In the case of Crimea's annexation, the Russian military campaign on the ground was accompanied by an active media campaign that undermined Ukrainian authorities and their efforts to protect the country. Russian information operations covered every layer of communication, targeting information assets in the physical and societal/cognitive domains. Information operations were applied from the strategic level - against the state institutions of Ukraine - to the tactical level in order to enable military actions by pro-Russian forces. From the early phase of the conflict until the annexation of Crimea, Russia controlled the information flow[28]. During the military operations in Crimea in March 2014, Russia managed to achieve information dominance. Russia controlled broadcast and print media, shaped the narrative in the social media and isolated Crimea from independent news from abroad[29]. The media-information isolation of Crimea was achieved by taking physical control of the internet and telecommunications infrastructure and by disrupting cable connections. Russia used all available means: fake news, troll campaigns, official government statements, YouTube videos, SMS messages, denial and deception, sabotage, cyber-attacks and narratives. Due to the information blackout, the target audience in Crimea shaped its perception mainly through Russian or pro-Russian media sources.

From the first day of the conflict, Russia denied direct involvement. When armed fighters - the so-called 'little green men' from Russia - appeared, both President Vladimir Putin and Defence Minister Sergei Shoigu denied the participation of Russian troops. In early March 2016, Ukraine reported damaged fiber-optic cables, jamming of naval communications and defacement of government portals. The mobile communications of government officials were compromised, and news portals suffered distributed denial of service attacks. Adding to that, a pro-Russian hacktivist group, Cyberberkut, managed to access phone recordings and electronic correspondence between Ukrainian, EU and US officials[30].

Russia used various media channels to distribute its disinformation and construct its narrative. These included both governmental and private TV channels (e.g., Rossiya 1, NTV, Russia Today, LifeNews), radio stations (e.g., Radio Mayak), mobile phone operators (e.g., KyivStar), Internet sources, including online publications (e.g., Itar Tass, RIA Novosti) and social media networks (e.g., YouTube, Facebook, Vk.com, odnoklassniki.ru). Russia also promoted the concept of Novorossiya (New Russia), as a new identity that would connect the breakaway regions of Donetsk and Luhansk, with Russia[31]. The separatist People's Republics of Donetsk and Luhansk had their own channels producing anti-Ukrainian

[26] Elias Götz and Jørgen Staun, "Why Russia attacked Ukraine: Strategic culture and radicalized narratives", *Contemporary Security Policy* 43 no. 3 (2022): 486.
[27] Vladimir Sazonov et.al. *Russian Information Campaign Against the Ukrainian State and Defence Forces* (Riga: NATO Strategic Communications Centre of Excellence, 2016).
[28] Jaintner, "Russian Information Warfare", 91.
[29] Giles, *The Next Phase of Russian Information Warfare*, 6-24.
[30] Jaintner, "Russian Information Warfare", 91.
[31] Treyger, Cheravitch and Cohen, *Russian Disinformation Efforts on Social Media*, 111.

propaganda (e.g., dnr-news.com, novorus.info). To conclude Russia managed to control the media environment and thereby manipulate the flow and content of news[32].

3.3 Information as an instrument of power: the case of the Russia-Ukraine War

On February 22 2022, Russia recognised the Donetsk People's Republic and the Luhansk People's Republic. Two days later Russia invaded Ukraine - according to the Kremlin's rhetoric 'a special military operation' - in order to demilitarize and denazify the regime and protect the ethnic Russian minority (humanitarian purpose). Since, most of the generic strategic narratives that appeared as part of the information operations in the case of Crimea's annexation (e.g. undermine Ukraine, divide the Western coalition supporting Kyiv) are also present in the ongoing war, we provide examples of only those narratives that are unique to the present case study. In particular, the most dominant narratives involved[33]:

- The division between the Western coalition (EU & NATO member-states)
- The deterioration of people's lives in the West, due to their governments involvement and support towards Ukraine
- The broader security concerns (energy, food and economic security) that the continuation of the conflict entails for the West
- The representation of the Ukrainian regime as a neo-nazi and fascist one and
- The negative portrayal of Ukrainian refugees

What follows is a selective list of examples that illustrate how Russia projected the above narratives.

[32] Sazonov, *Russian Information Campaign Against the Ukrainian State and Defence Forces*.

[33] See selectively the daily updates of Russian disinformation in Ukraine World, https://ukraineworld.org/articles/infowatch/RU-disinfo as well as EUISS Analysis, *The Kremlin's Information War 2.0. An analysis of trends in Russian official communication on Ukraine* (Paris: European Union Institute for Strategic Studies, June 2022), https://twitter.com/EU_ISS/status/1545324979138580480 and Recorded Future, *Russian information operations aim to divide the western coalition on Ukraine*, Threat Analysis - Russia, 7 July 2022, https://www.recordedfuture.com/russian-information-operations-divide-western-coalition-ukraine

- On March 2022, Fontanka, an independent news organization based in St Petersburg discovered Cyber Front Z, a Telegram[34] troll farm that was recruiting people to post 200 pro-Russian comments every day to platforms including Instagram and YouTube[35].

- On May 2022, the websites Global Research and UNZ Review published articles by the same author, who claimed that the UK government is financially supporting the Nazi regime in Ukraine[36].

- On May 2022, pro-Russian Telegram sources as well as RIA Novosti exploited the historic territorial claims between Poland and Ukraine and claimed that Poland was planning to take advantage of the situation and take control over Ukrainian territory near its borders[37].

- Russian news and pro-Telegram sources portrayed negatively Ukrainian refugees and indirectly blamed them for worsening living standards in the country that accepted them (note

[34] Both Russia and Ukraine used various social media platforms like VKontakte, Twitter, Instragram and messaging apps like WhatsApp, Signal, Viber and Facebook Messenger to promote their information operations, but Telegram stands out as the most popular one, since it enables its users to create groups of up to 200.000 members. See Christian Perez, "Information Warfare in Russia's War in Ukraine. The role of social media and artificial intelligence in shaping global narratives", *Foreign Policy,* August 22, 2022, https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/

[35] Alexander Martin, "Ukraine war: Britain accuses sick Russian troll factory of plaguing social media with Kremlin propaganda", *Sky News,* May 1, 2022, https://news.sky.com/story/ukraine-war-britain-accuses-sick-russian-troll-factory-of-plaguing-social-media-with-kremlin-propaganda-12603200

[36] Brett Redmayne-Titley, "Ukraine's Nazi connection and the British national cover-up", *The UNZ Review*, May 21, 2022, https://www.unz.com/article/ukraines-nazi-connection-and-the-british-national-cover-up/ and Brett Redmayne-Titley, "History of Ukraine's Nazi connection", *Global Research*, May 23, 2022, https://www.global-research.ca/ukraine-nazi-connection-british-national-cover-up/5781054

[37] Recorded Future, *Russian information operations aim to divide the western coalition on Ukraine*, 5 and RIA Novosti, "Poland moves to seize the western territories of Ukraine, says Patrushev", May 31, 2022, https://ria.ru/20220531/patrushev-1792037525.html

that Poland has accepted millions of Ukrainians since February)[38]. The scope of such rhetoric was to amplify anti-migrant policies often associated with both conservative political parties and ultra-right groups. Furthermore, MK reported on June 2022, that Russian citizens living in Poland had been denied access to jobs and housing and that they had been attacked or bullied by Ukrainian refugees in public places[39].

- On June 2022, in an article published by the pro-Russian online magazine New Eastern Outlook (regarded to be under the direction of the Russian SVR)[40] it was argued that NATO is determined to defeat Russian, even if that leads millions of people to starvation. Likewise, according to the author, the EU instead of investing on a peace agreement is exploiting this situation in order to undermine African nations[41].

In sharp contrast to the case of Crimea, Ukraine responded to the Russian invasion of February 2022, not only in military terms, but also by deploying a full range of information operations. The targeted audiences of these operations were the Ukrainian population and troops, the Russian government, population and troops operating in Ukraine and finally the international community. The most dominant narratives were the following[42]:

- The moral support to the Ukrainian population and its troops (e.g. the inherently just cause of Ukrainian self-defense, the firmness of Ukrainian resistance, emphasis given on boosting national unity, fighting spirit and resilience)
- The demoralization of the Russian invasion (e.g. illegal actions conducted by Russian troops against Ukrainians, the barbarity of Russian soldiers, the futility of fighting against highly motivated Ukrainian soldiers and citizen-volunteers)
- The isolation and punishment of Russia for the alleged war crimes (e.g. imposing and hardening of sanctions)
- The desperate need for international support (financial, military, diplomatic) to Ukraine

[38] Notes from Poland, "Russia using disinformation to stir hostility between Ukrainians and Poles, warn security services", May 31, 2022, https://notesfrompoland.com/2022/05/31/russia-using-disinformation-to-stir-hostility-between-ukrainians-and-poles-warn-security-services/ and Sputnik International "Belgian Families Hosting Ukrainian Refugees Complain of Exhaustion, Social Worker Says", June 7, 2022, https://sputniknews.com/20220607/belgian-families-hosting-ukrainian-refugees-complain-of-exhaustion-social-worker-says-1096094438.html

[39] MK, "Russians who arrived in Poland ended up in hell: "It's scary to talk in the street", June 7, 2022, https://www.mk.ru/social/2022/06/07/priekhavshie-v-polshu-russkie-okazalis-v-adu-strashno-razgovarivat-na-ulice.html?utm_source=yxnews&utm_

[40] Recorded Future, *Russian information operations aim to divide the western coalition on Ukraine*, 9.

[41] Phil Butler, "NATO's Mission Imperative: Break Russia Even If Millions Worldwide Perish", *NEO – New Eastern Outlook,* June 2022, https://journal-neo.org/2022/06/02/nato-s-mission-imperative-break-russia-even-if-millions-worldwide-perish/

[42] Michael Butler, **"**Ukraine's information war is winning hearts and minds in the West**"**, *The Conversation,* May 12, 2022, https://theconversation.com/ukraines-information-war-is-winning-hearts-and-minds-in-the-west-181892

Ukraine managed to communicate its side of the story better that Russia. To begin with, President Volodymyr Zelenskyy, acting as a media star and appearing in military-style clothing has framed the war as a battle between the Ukrainian David standing up to the Russian Goliath. Besides Zelenskyy, Ukrainian officials and individual citizens flood social media with words and images about their resistance to the invader[43]. In the first days of the war, the Ukrainian government encouraged its citizens to resist, to block the streets so that Russian troops cannot advance and to demonstrate that they are not welcome. Furthermore, Ukraine set up web pages containing pictures and information about Russian prisoners of war, in an effort to demoralize the Russian population with photos and videos of captured Russian soldiers. The external target audience, meaning the international community, was obviously more sympathetic to the Ukrainian narrative, than to the Russian one. Kyiv also successfully used fact-checker groups to undermine Russia's rhetoric and warned its citizens and the international public opinion of potential Russian false flag operations. To conclude, Ukraine dominated on the information battleground and by gaining international support, managed to translate this success into effective defense of its territory.

3.4 Lessons learned on the utility of information operations

It is important to note, although not within the scope of the present paper, that Russia has employed information instruments long before the annexation of Crimea in 2014. From the late 1990s, but more aggressively in the years following the Orange Revolution in Ukraine, the Kremlin used media to transmit narratives that questioned Crimea's connection with Ukraine, in cultural and historic terms and

[43] Seib, "Why Russia is losing the information war in Ukraine".

stressed Crimea’s strong ties to Moscow. Likewise, Kremlin’s soft power tools constantly highlighted Russia’s scientific achievements and high standards of living and devalued Ukraine[44].

In both case studies examined, the objectives of the Russian information operations were the same at the strategic level, although differed at the tactical one. In particular, their objectives were, and still are regarding the ongoing war, the following:

- To demoralize the Ukrainian public and its armed forced
- To distort the facts/truth about historical (e.g. the legality of the Soviet Union’s decision to transfer control of Crimea to the Ukrainian Soviet Socialist Republic in 1954) and contemporary events (e.g. the nazification of the existing regime)
- To establish support for Russian actions in Ukraine among Ukrainian audiences
- To establish support for Russian actions in Ukraine among Western audiences

The record of Russia’s information operations is rather mixed. Taking over Crimea without any military confrontation demonstrated the utility of the informational campaign in operational terms, but also the centrality of these concepts in the Russian strategic thinking. On the other hand, this success was limited in Russia and Crimea, and the relevant target audiences (Russians and Russophones in Crimea). Outside of these areas, where the citizens were largely not deprived of alternative information sources, the Kremlin failed to impose its viewpoints[45].

Furthermore, although in tactical and operational terms, the information operations in Crimea were a success, in strategic terms the story is much different. Crimea served as a wake-up call not only for Ukraine, but also for the rest of the West. Crimea and the events that followed until the invasion in February 2022 polarized part of the West against Russia and eventually led to NATO’s enlargement. Adding to that, most of Russia’s tools and methods were easily identified by the targeted audiences. Disinformation campaigns erode over time as more and more evidence that is factual is revealed to negate lies and falsification. In the case of the February 2022 invasion in Ukraine, Russia did not enjoy the advantage of surprise and its information operations playbook seemed outdated. This again only partly explains the failure of the Russian information operations in the second case study.

We have to acknowledge that Ukraine was expecting a similar information campaign and had devised its plans in advance. In sharp contrast to the Crimean case where Moscow capitalised on the democratic environment in order to spread its narratives unhindered, in 2022 Russian media faced restrictions and in some cases, like that of Russia Today, were even banned from broadcasting. Furthermore, social media platforms characterised Russia’s state-owned media content as unreliable.

[44] Michelle Grisé et.al. *Rivalry in the Information Sphere. Russian Conception of Information Confrontation* (Santa Monica: RAND, 2022), 90-92.

[45] Maria Snegovya, *Putin’s Information Warfare in Ukraine. Soviet origins of Russia’s hybrid warfare* (Washington DC: Institute for the Study of War, 2015).

4. Policy recommendations for NATO

The question that inevitably arises is what can be done to counter such operations? Any effort to counter Russia's information operations requires a comprehensive approach that involves state agencies, collective actions within NATO, cooperation with the private sector and the active involvement of the media in investigative journalism projects and the construction of counter-narratives[46]. NATO's member-states can respond to information campaigns with defensive or offensive measures. In particular, defensive measures are overt and aim to safeguard a state's information domain, whereas offensive ones are covert and aim to target the enemy's information domain. Striking a balance between defensive and offensive measures is not an easy task, for reasons that mainly have to do with the way a liberal democracy functions. Paradoxically enough, democracies have to tolerate some propaganda in order to stand up for democratic values. Democracies have to draw a line between legitimate expressions of freedom of speech, on the one hand, and foreign interference that triggers political upheavals. However, the dividing lines between ordinary people expressing their views and state sponsored trolls can sometime be vague. To what extent should democracies value freedom of speech and thereby enable the spread of disinformation and fake news? One defensive measure, for example, is censorship of the Russian media. This option is very unpopular within the Alliance. Any form of censorship would create a boomerang effect, since it would legitimize the Russian narrative. Likewise, an offensive measure is the employment of counter information warfare campaigns, in order to infiltrate and manipulate the Russian information domain. Again, such an option is not desirable in liberal de-

[46] Maria Hellman and Charlotte Wagnsson, "How can European States respond to Russian information warfare? An analytical framework", *European Security* 26, 2 (2017): 153-170.

mocracies that aim to protect and project the truth. Despite the above setbacks, NATO and its member-states cannot be apathetic when they spot deliberate cases of fake news and disinformation. After all, the protection of democracy does not go beyond the scope of NATO[47]. Thus, the Alliance should consider the following:

- To begin with, the Alliance and its member-states should engage in a public debate, clearly state the false arguments that have been used, and raise public awareness. Adding to that, instead of censoring, governments should activate independent regulatory agencies that could take proper actions against media organizations that act as agents of influence.

- In order to counter Russian information operations, governments need to engage all relevant agencies in the areas of defense, foreign policy, internal security, public diplomacy and strategic communication. No state, no matter how strong, can counter this challenge on its own. The exchange of information and best practices between the member-states of the Alliance and other parties is a prerequisite.

- Media and internet literacy is another tool that NATO needs to fully utilize. Since the public audience is the main target of such campaigns, educating the public in identifying propaganda is imperative[48]. Likewise, in an era when social media dominate the discourse, governments need to invest in internet literacy in order to confront hostile narratives. Tailor-made courses should be offered to government officials and journalists to educate them in how to identify disinformation and trace the origins of fake reports.

- Information warfare is a battle of narratives. Therefore, the combatant with the most convincing narrative gains influence. In contrast to Russia, which enjoys an integrated approach, collective entities like NATO will always lack a common narrative. Thus, emphasis must be given in synchronizing efforts and narratives, based on the common values and objectives of the Alliance.

- The battle for hearts and minds is conducted both at home and abroad. In states that have a Russian minority, governments should engage with this target audience in the Russian language through news programs, talk shows, and culture and entertainment programs. In the past, BBC World, Voice of America and Radio Free Europe have served as instruments of soft power, but the media environment is now more complicated that it was during the Cold War. The Alliance needs to fund tailored Russian language programs that deconstruct the hostile narratives that have been put forward by Russia[49].

- Technology, too, can assist in identifying and countering the spread of disinformation. Think-tanks and civil society organizations like the Atlantic Council's Digital Forensics Lab, StopFake.org and the Authoritarian Interference Tracker by the German Marshall Fund of the United States, have developed social media algorithms to trace the dissemination of fake news. Likewise, NATO and its member-states should invest heavily on open-source intelligence analysis,

[47] In relation to this, see the discussion about the establishment of a Center for Democratic Resilience at NATO, https://nato-pa.foleon.com/coordination-centre-on-democracy-resilience/the-case-for-a-center-for-democratic-resilience-in-nato/a-blueprint-for-the-center-for-democratic-resilience-in-nato

[48] In Finland, media literacy programs have already been added to the education's system curricula.

[49] A good example towards this direction is the United States Agency for Global Media (USAGM), which delivers Russian language programs in Ukraine, Moldova, Belarus and Kazakhstan.

big data analytics and predictive analytics models and algorithms that offer an early warning of such malicious activities.

- Finally, the most suitable way to face Russia's information warfare is to identify the disinformation and debunk it by presenting rational arguments supported by real evidence. In order to achieve this, the Alliance and its partners need not only to apply all the above measures, but also to gain a better knowledge of Russia. The development of expertise on Russian culture, history, modern politics and strategic thinking, will enable scholars, government officials and decision makers to gain a better understanding of Russian policy[50]. The Alliance should monitor more closely Russian-language sources and military-academic journals in order to understand better Russian intentions and perceptions in the information domain.

5. Conclusions

The paper clearly established the importance of information as an instrument of power and highlighted the various means, with which information operations are conducted. Though the direct results of such operations are hard to measure, it seems that in both cases examined, the Kremlin managed to construct and broadcast strategic narratives that favored its policy goals, as well as to penetrate Western societies and influence public opinion. The degree of success varies. In the case of Crimea's annexation, Russia had the advantage of strategic surprise and managed in information terms to isolate the specific region. Ukraine on the other hand was ill prepared to counter such a sophisticated information campaign and distribute effectively its counter-narratives. In the second case, that of the Russia-Ukraine war that is still ongoing, the record is rather mixed. In this case, Ukraine, and the West in general, were not taken by surprise and managed to identify Russia's playbook of information operations. On the other hand, Russia succeeded in securing its domestic audience by disconnecting from the global Internet. This development made the Russian information space resilient and created an asymmetry that favored the Kremlin's political objectives. In terms of reaching and convincing western audiences, Russia scored a low record, but seemed to be more successful in exploiting ambiguity and distrust in the social media and thereby undermine the truth and the very idea of objective reporting.

Confronting Russia's information operations is not an easy task. In the battle of narratives, liberal democracies should respect the pillars of democracy and rule of law while simultaneously protect the democratic order from foreign influence. Over the past years, the establishment of institutions like: StratCom (NATO's Strategic Communications Centre of Excellence), East StratCom Task Force (within the European External Action Service),[51] EU Hybrid Fusion Cell (within the EU Intelligence and Situation Centre), and the European Centre of Excellence for Countering Hybrid Threats, are developments that point to the right direction and offer tools to respond to Russia's disinformation campaign[52]. Nevertheless, an effective counter-strategy requires an integrated approach: an empowered civil society, synergies between NATO, the EU and other partners (e.g. academic, social media platforms), as well as tailored communications products that identify disinformation and project the truth. Such an all-

[50] Grisé, *Rivalry in the Information Sphere*, 100.

51 The East StratCom Task Force publishes two weekly newsletters, the *Disinformation Review* and the *Disinformation Digest,* that offer a systematic overview of cases of disinformation. Such publications and their social media accounts collect and report cases of disinformation and inform journalists.

[52] Sijbren De Jong et.al. *Inside the Kremlin House of Mirrors: How Liberal Democracies can counter Russian Disinformation and Societal Interference* (Hague: The Hague Center for Strategic Studies, 2017): 56-72.

encompassing approach will ensure the necessary balance between the functioning of liberal democracy and the protection of societal cohesion. Fighting propaganda with propaganda is simply not an option. It is only the truth that sheds light on the darkness.

References

Allen, T.S and A.J. Moore, “Victory Without Casualties: Russia’s Information Operations”, *Parameters* 48, 1 (2018): 59-71.

Andrew, Christopher and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999).

Armistead, Leigh (ed.) *Information Operations Matters. Best Practices* (Washington DC: Potomac Books, 2010).

Bērziņš, Jānis, “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defence Policy”, *Policy Paper* 2 (Riga: National Defence Academy of Latvia, Center for Security and Strategic Research, April 2014).

Butler, Michael, “Ukraine’s information war is winning hearts and minds in the West”, *The Conversation,* May 12, 2022, https://theconversation.com/ukraines-information-war-is-winning-hearts-and-minds-in-the-west-181892

Butler, Phil, “NATO’s Mission Imperative: Break Russia Even If Millions Worldwide Perish”, *NEO - New Eastern Outlook,* June 2022, https://journal-neo.org/2022/06/02/nato-s-mission-imperative-break-russia-even-if-millions-worldwide-perish/

Chivvis, Christopher, “Hybrid War: Russian Contemporary Political Warfare”, *Bulletin of the Atomic Scientists* 73, 5 (2017): 316-321.

Darczewska, Jolanta, *The Devil is in the details: Information Warfare in the Light of Russia’s Military Doctrine* (Warsaw: Centre for Eastern Studies, 2015).

De Jong, Sijbren et.al. *Inside the Kremlin House of Mirrors: How Liberal Democracies can counter Russian Disinformation and Societal Interference* (Hague: The Hague Center for Strategic Studies, 2017).

EUISS Analysis, *The Kremlin’s Information War 2.0. An analysis of trends in Russian official communication on Ukraine* (Paris: European Union Institute for Strategic Studies, June 2022), https://twitter.com/EU_ISS/status/1545324979138580480

Fridman, Ofer, “The Russian Perspective on Information Warfare: Conceptual roots and politicisation in Russian academic, political and public discourse”, *Defence Strategic Communications* 2 (2017): 61-83.

Galleoti, Mark, “The mythical ‘Gerasimon Doctrine’ and the language of threat”, *Critical Studies on Security* 17, 2 (2019): 157-161.

Giles, Keir, *The Next Phase of Russian Information Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016).

Glantz, David, *Surprise and Maskivorka in Contemporary War* (Kansas: Fort Leavenworth, Soviet Army Studies Office, Army Combined Arms Center, 1988).

Götz, Elias and Jørgen Staun, “Why Russia attacked Ukraine: Strategic culture and radicalized narratives”, *Contemporary Security Policy* 43 no. 3 (2022): 482-497.

Grisé, Michelle et.al. *Rivalry in the Information Sphere. Russian Conception of Information Confrontation* (Santa Monica: RAND, 2022).

Hellman, Maria and Charlotte Wagnsson, “How can European States respond to Russian information warfare? An analytical framework”, *European Security* 26, 2 (2017): 153-170.

Jaintner, Margarita, “Russian Information Warfare: Lessons from Ukraine”, in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, 87-94. (Tallinn: NATO CCD COE 2015).

Khaldarova, Irina, “Brother or ‘Other’? Transformation of strategic narratives in Russian television news during the Ukrainian crisis”, *Media, War & Conflict* 14 no.1 (2021): 3-20.

Lilly, Bilyana, *Russian Information Warfare* (Annapolis: Naval Institute Press, 2022).

Martin, Alexander, “Ukraine war: Britain accuses sick Russian troll factory of plaguing social media with Kremlin propaganda”, *Sky News,* May 1, 2022, https://news.sky.com/story/ukraine-war-britain-accuses-sick-russian-troll-factory-of-plaguing-social-media-with-kremlin-propaganda-12603200

Matthews, Miriam et.al. *Understanding and defending against Russia’s malign and subversive information efforts in Europe* (Santa Monica: Rand, 2021).

MK, “Russians who arrived in Poland ended up in hell: “It’s scary to talk in the street”, June 7, 2022, https://www.mk.ru/social/2022/06/07/priekhavshie-v-polshu-russkie-okazalis-v-adu-strashno-razgovarivat-na-ulice.html?utm_source=yxnews&utm_

Mölder, Holger et.al. *The Russian Federation in Global Knowledge Warfare. Influence Operations in Europe and its Neighborhood* (Cham: Springer, 2021).

Notes from Poland, “Russia using disinformation to stir hostility between Ukrainians and Poles, warn security services”, May 31, 2022, https://notesfrompoland.com/2022/05/31/russia-using-disinformation-to-stir-hostility-between-ukrainians-and-poles-warn-security-services/

Perez, Christian, “Information Warfare in Russia’s War in Ukraine. The role of social media and artificial intelligence in shaping global narratives”, *Foreign Policy,* August 22, 2022, https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/

Recorded Future. *Russian information operations aim to divide the western coalition on Ukraine*, Threat Analysis - Russia, July 7, 2022, https://www.recordedfuture.com/russian-information-operations-divide-western-coalition-ukraine

Redmayne-Titley, Brett, “History of Ukraine’s Nazi connection”, *Global Research*, May 23, 2022, https://www.globalresearch.ca/ukraine-nazi-connection-british-national-cover-up/5781054

Redmayne-Titley, Brett, “Ukraine’s Nazi connection and the British national cover-up”, *The UNZ Review*, May 21, 2022, https://www.unz.com/article/ukraines-nazi-connection-and-the-british-national-cover-up/

RIA Novosti, “Poland moves to seize the western territories of Ukraine, says Patrushev”, May 31, 2022, https://ria.ru/20220531/patrushev-1792037525.html

Sazonov, Vladimir et.al. *Russian Information Campaign Against the Ukrainian State and Defence Forces* (Riga: NATO Strategic Communications Centre of Excellence, 2016).

Seib, Philip, “Why Russia is losing the information war in Ukraine”, University of Southern Carolina, Center on Public Diplomacy, https://uscpublicdiplomacy.org/blog/why-russia-losing-information-war

Sherman, Justin, “Reassessing RuNet. Russian Internet isolation and implication for Russian cyber behavior”, *Atlantic Council*, Issue Brief, 12 July 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/

Snegovya, Maria, *Putin’s Information Warfare in Ukraine. Soviet origins of Russia’s hybrid warfare* (Washington DC: Institute for the Study of War, 2015).

Sputnik International, “Belgian Families Hosting Ukrainian Refugees Complain of Exhaustion, Social Worker Says”, June 7, 2022, https://sputniknews.com/20220607/belgian-families-hosting-ukrainian-refugees-complain-of-exhaustion-social-worker-says-1096094438.html

Thomas, Timothy, “Russia’s 21st Century Information War: Working to Undermine and Destabilize Populations”, *Defence Strategic Communications* 1, 1 (2015).

Thomas, Timothy, “Russia’s Information Warfare Strategy: Can the Nation Cope in Future Conflicts?”, *The Journal of Slavic Military Studies* 27 (2014): 101-130.

Thornton, Rob, “The Changing Nature of Modern Warfare: Responding to Russian Information Warfare”, *RUSI Journal* 160, 4 (2015): 40-48.

Thornton, Rob and Marina Miron, “Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow’s Strategic Thinking”, *The Cyber Defence Review* 7, 3 (2022): 117-135.

Treyger, Elina, Joe Cheravitch and Raphael S. Cohen, *Russian Disinformation Efforts on Social Media* (Santa Monica: Rand, 2022).

Van Herpen, Marcel, *Putin’s Propaganda Machine: Soft Power and Russia’s Foreign Policy* (Lanham: Rowman & Littlefield, 2016).

Walker, Christopher, “The Authoritarian Threat. The hijacking of ‘Soft Power’”, *Journal of Democracy* 27, 1 (2016): 49-63.

Interpol database
Console
Neural Network Tracing

OPEN PUBLICATIONS

INFORMATION AS AN INSTRUMENT OF POWER

LESSONS LEARNED FROM THE WAR IN UKRAINE