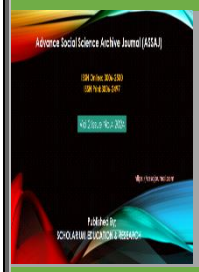

Advance Social Science Archive Journal
Available Online: https://assajournal.com
Vol.3 No.1,January-March,2025.Page No.824-837
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

DECIPHERING RUSSIAN INFORMATION WARFARE: LESSONS FROM GEORGIA TO CRIMEA AND UKRAINE

Muhtasim Afridi
BS Graduate in Strategic Studies, National Defence University, Islamabad
Email: muhtasimafridi166@gmail.com

ABSTRACT

The Third Industrial Revolution gave birth to computers and electronics thus strengthening communication networks. The increased flow of information across the globe enhanced research and development; however, the technology-savvy nations became more vulnerable to 'Information Warfare' an umbrella term for cyberwarfare, disinformation, propaganda, and psychological operations. This type of warfare is primarily based on technology and information systems. The Cold War period saw a huge loss of human life and resources – given such a high cost of resorting to conventional war, states realised the importance of having control over cyberspace. A profound application of information warfare is found in Russia's conduct of war – the country has evolved to familiarize itself with information warfare tactics. In the 21st century, the Russian leadership has integrated 'information superiority' into its military doctrines and strategies. This paper provides insights into the means and methods used under information confrontation. It sets out to examine how Russia conducts information warfare and has consistently developed its information warfare doctrine over the past two decades. By referring to three conflicts including the Georgian crisis of 2008, the Crimean annexation in 2014 and the ongoing conflict in Ukraine, it shed light on various aspects of Russian information warfare. Though Russia achieved concrete gains in the Georgian crisis and during the annexation of Crimea, the paper underscores why Russia fell short of meeting expectations in the invasion of Ukraine.

Keywords: Information warfare, cyberwarfare, disinformation, propaganda, social media

Introduction

States are very practical in terms of cost and benefit when deciding to wage a war. With rapid advancements in technology, lethality has increased – particularly with the advent of nuclear weapons the risk of nuclear exchange soars high. In such a scenario resorting to a conventional war has become extravagant and absorbent. Post 9/11 the phenomenal upsurge of non-state militant groups and their widespread use as proxies

viz-a-viz the averseness of states to go for a full-fledged war has further condensed the ground for the likelihood of conventional war. As stated earlier, states are rational in decision-making, hence they go for an alternative means to achieve a strategic advantage in a conflict. Here comes the play of information warfare which aims to disorient and divide the enemy's population by the use of propaganda and psychological operations. So far Russia has mastered the information warfare strategy – given their consistent development in this domain. The country's top leadership is well aware of the importance of information in controlling and manipulating the domestic as well as international audience.

In the Russo-Georgian War in 2008, overtaken by the robust Georgians in information warfare, Russia realised the advantage of having control over the online environment (Iasiello, 2017). Thus, over the period, the country has evolved to familiarise itself with the fundamentals of cyberspace. Due to the wider use of social media platforms and the increased flow of information together with its access to the larger internet community has made netizens vulnerable to psychological influence. Learning from its past experiences Russia perfected the information tactics and developed effective and robust communication networks. A decent illustration of the Russian information warfare strategy is found in the annexation of Crimea in 2014 when the state's authorities used social and mainstream media to manipulate and control the Crimean population. Within a matter of weeks, Russia was able to occupy Crimea without hitting the headlines or making the international community realise about the events happening inside the territory. Following the footprints of the Crimean crisis, Russia started applying the same tactics in the Ukraine conflict; however, with a varying degree and in a slightly different manner. This paper focuses on the evolving nature of Russian information warfare while giving reference to the distinct case studies of Georgia, Crimea, and Ukraine, and also examines the relevance of information warfare in contemporary times.

Making Sense of Information Warfare

Information warfare is as old as the war itself. The ancient theorists and military strategists such as Genghis Khan, Mao Tse Tung, Jomini, Ho Chi Minh, the Médicis, Von Clausewitz, Che Guevera, Slobodan Milosovic and Fidel Castro all practised information warfare. It is only because of technology that past and present warfare is different in some manner, however, the overall nature of war remains the same. Given the rapid advancement in technology, the intensity and application of information warfare have increased over time, and has become a key component of military planning (Khan, 2012).

'Information warfare' in the broader sense is a constituent of 'Hybrid warfare' a term which was first used in the aftermath of the 2006 conflict between Israel and Hezbollah.

As a fragment of the 'cross-domain' war concept, hybrid warfare entails unconventional approaches, i.e., conceptually discrete features deployed synergistically through a concerted operation designed to disorient and paralyse the adversary without turning to a full-scale conventional war (Shah & Ehsan, 2022). Similarly, information warfare contains non-kinetic means including propaganda, disinformation, denial and deception. These elements remain at the heart of information warfare and provide an upper hand over the enemy. The nature of such activities is less destructive and works particularly as an influencing agent. Even with less firepower against an adversary, a piece of credible information and a strong communication system can increase the probability of victory (Jaitner & Mattsson, 2015). As described by Sun Tzu in the book "The Art of War", "All warfare is based on deception" (Tzu, 2007) and "The best victory is to subdue your enemy without resorting to actual force," (Tzu, 2007) information warfare functions in the same manner – it is based on psychological operations, requires fewer resources and does not necessitate the use of actual force.

To further clarify the concept, information warfare can also be referred to as a war without confrontation, or war short of direct conflict. This type of warfare is primarily led by employing tools such as technology and information. Contrary to conventional wars consisting of soldiers on the ground, guns, artillery, tanks, fighter aircraft, etc., information warfare entails tools such as cyberattacks, propaganda, artificial intelligence, and social engineering (Abbott, 2010).

Multiple authors have varying views on information warfare; however, Grumman has stated that "the ability to manipulate, deceive, distort, and interrupt enemy's information structure while concurrently safeguarding your own" refers to information warfare (Stephenson, 1999). In general terms, information warfare is defined as, "a unified and coordinated blend of virtual and physical actions aimed to influence individuals, organizations, and states into performing or refraining from performing certain actions so that your ultimate objective is achieved, while synchronously averting your opponent from doing the same to you (Jones et al., 2002)."

Two Russian military experts argued in 2013 that "the key elements to dominate the new-generation war will be: 'information tactics and psychological operations', where militaries will tend to accomplish strict control over their forces and weaponry and befuddle the armed personnel and population of adversary both morally and psychologically. As information technology transforms, it will rule the methods of war at large, hence, information tactics and psychological operations will set down the foundation for victory (Porkoláb, 2024)." Given the importance of such tactics, Russia utilises information warfare to influence the beliefs, thoughts, and actions of specific

targeted groups aimed to achieve its strategic objectives within the adversary's territory.

Russian Information Warfare Doctrine

Russia's academic perspective and national policy on information as a means of war give a significant context for the state's conduct of information operations. The country's top leadership considers information superiority integral to its military doctrines and strategies. In a conversation, a Russian military expert and retired Colonel Viktor Murakhovsky bluntly proclaimed that practically Russia never faced defeat against its adversaries over the period in history, except when its population was subjected to psychological influence (Wilde & Sherman, 2023). Far from bragging, this statement is widely common throughout Russia's military planning and practices, which recognizes the importance of information in national security, domestic control, conflict abroad, and wider geopolitical competition.

Since the ascent of Vladimir Putin in December 1999, Russia has not formed any unified doctrine on its information warfare, rather the government has issued a sequence of military doctrines, strategies and policy concepts. These policy and strategy documents illustrate the Kremlin's thinking of the online environment and establish operational and strategic urgencies for Russia's information apparatus (Wilde & Sherman, 2023). The Doctrine of Information Security published by the Russian Federation in 2000 professed the substantial dependence of state safety on the level of information security and highlighted that this dependence is destined to surge identically with technological advancements (Federation, 2000). Apart from stressing global competition for information technology, the doctrine also enlisted countermeasures against political, economic, and military threats to the Russian Federation in the realm of information (Federation, 2000).

Published in the same year, the Russian Military Doctrine incorporated similar aspects of information warfare. It focused on securing the Russian Federation and its allies from information and psychological operations. The primary internal threats to the federation included rebellion against the constitutional order, exertions by separatist, religious, extremist nationalist, and terrorist movements to subvert Russia's domestic political stability, and any operations with the intent to destroy the central organs of state or any economic or military facilities concerned to vital information setup (Pietkiewicz, 2018).

In the following years, Moscow released several other policy documents related to information security which include the Foreign Policy Concept 2008, the Military Doctrine 2010, the Military Doctrine 2014, the 2015 National Security Strategy, the Foreign Policy Concept 2016, the Information Security Doctrine 2016, and the National

Security Strategy of 2020 and 2021. These documents emphasized the notion of information safety as central to national security and the state's foreign policy.

For instance, the 2020 National Security Strategy of Russia while assessing future threats specified that worldwide information warfare will intensify – hence the nationalist and separatist movements will continue to haunt and become a primary danger to the state. The strategy envisages eradicating these threats by broadcasting "truthful" information to state citizens and promoting and developing indigenous media platforms (Jaitner & Mattsson, 2015). Suffice to say, that this is evident due to Russia's strict control of larger media channels such as Russia Today (RT) and Sputnik. The wider role of RT and Sputnik in the annexation of Crimea in 2014 is a logical consequence of such approaches. Now, consider a state with a formidable information history, to what extent must it have evolved its information systems? Russia's continuous application of information operations in conflicts helped the state to strengthen information security mechanisms and master information warfare tactics. The following case studies illustrate how Russia's understanding of information confrontation has evolved in the 21st century.

The 2008 Russo-Georgian War

Russia and Georgia fought a brief conflict in 2008 primarily based on information warfare. Both states employed kinetic and non-kinetic offensives, i.e., synergistically using conventional military forces vis-a-vis cyberattacks, propaganda and, denial and deception efforts. The Georgian conflict demonstrates a larger picture of Russia's thinking and conduct of technical and psychological operations employed jointly with military attacks (Thomas et al., 2010). This conflict was the first of its kind where conventional military operations and cyberattacks functioned simultaneously. The technical offensives included hacking of websites and denial of service attacks against the Georgian government, media outlets, and financial institutions, together with public and private entities. The attacks were executed in a very sophisticated manner, thus effectively denying citizens access to 54 web pages associated with government, communications, and finance (Oltsik, 2009). While some speculated Russia's involvement in the attacks, there was no concrete evidence to prove the claims because hackers are hard to track, they operate like ghosts.

The Russian intelligence agencies also engaged in synchronized psychological operations – including strict information control, propaganda and disinformation campaigns, with a varying degree in contrast to the Georgian information confrontation. Russia was engrossed on disseminating its narrative to the international audience through television footage thereby justifying its intervention. The key themes delivered by the Russian Federation portrayed the United States' Western allies and Mikheil Saakashvili the then Georgian president as assailants and invaders. On the

contrary, the Russian media described Russia as the saviours and defenders of Georgian citizens (Cohen & Hamilton, 2011). By broadcasting interviews with military spokesmen consistently, Russia attempted to manipulate the local population and distributed news which showed that Russian troops were protecting the Russian citizens against the Georgian atrocities. The operations initially proved effective; a CNN poll showed that 92% of respondents at that time supported Russian intervention believing it to be justified (Levine, 2008).

Instead of kneeling, Georgians launched a counter-disinformation campaign using state-owned media. The Georgian government also demanded assistance from professional private firms dealing with public relations to endorse its narrative and limit the effects of Russian propaganda. In addition, while the cyber-attacks by Georgia proved less successful at large, they were effective in shutting down some Russian services. Many security experts observed Russia's success in the whole conflict, however, a Russian military commander Anatoliy Tsyganok believed that at the beginning of information offensives, Georgia was at the forefront, but it lost at the end (Thomas et al., 2010). In terms of information-based technologies, Georgia had an edge over Russia. Therefore, after receiving a bulk of criticism in the aftermath of the conflict, the Russian military brought several key reforms to its broader defence framework.

Analysis of Russian Information Operations in Crimea

The invasion of Crimea is another key event which served as a ground for Russian information tactics. The invasion was a coordinated effort of all the Russian authorities including its intelligence network, military troops, media entities, and several pro-Russian groups in Ukraine, whereby using instruments such as propaganda, information collection, and media monitoring to gain control over the virtual space (Konończuk, 2013). The Russian leadership had set the stage early before 2014; when it deployed 'GRU', an intelligence service of Russia, in parts of Crimea, and tasked them to gain long-term residency in the territory by using bogus Ukrainian companies (Bouwmeester, 2021). Among other groups were the GRU 'fire-starters', who were tasked to create mess and chaos, spread disinformation and provoke incidents to destabilise the state of affairs in Ukraine – ultimately, the GRU gradually increased its influence (Bouwmeester, 2021). Just like in the case of Georgia, Russia used information tactics in Ukraine, but this time in a more advanced form, given the exact timing of cyberattacks against the enemy's key infrastructures, which has always been the priority in wars to gain maximum advantage (Allegri, 2023).

In the midst of 2013, Russia launched 'Operation Armageddon' which targeted the government officials of Ukraine along with the military officers and law enforcement officials intended to get hold of their secret information. The operation was initiated

soon when the European Union (EU) and Ukraine engaged in negotiations for economic cooperation. A highly sophisticated computer virus named "Snake" was transmitted by Russian hackers into the Ukraine Prime Minister's office and various Ukrainian embassies in other countries (Allegri, 2023). Such advanced spying methods helped the Russian authorities navigate through the strategic thinking of Ukraine. Furthermore, the Russian officials exploited certain journalists having a wide reach to understand public view, which would eventually help the Russian authorities to identify rebels and then circulate disinformation and pro-Russian texts to them utilizing different channels. Likewise, cyber operations proved very effective in stealing information including the phone chats between the US and Ukrainian officials (Allegri, 2023).

A real mess was created in November 2013 when the then-President of Ukraine Viktor Yanukovych decided not to sign an agreement which would have increased the chances of Ukraine's integration with the European Union (Zelinska, 2017). The decision was followed by massive but peaceful demonstrations around the country, specifically in Maidan or Independence Square, which continued and entered into 2014. The security forces began to storm the demonstrators, however, the number of protestors only doubled up in reaction and transformed into what was labelled "Revolution of Dignity" (Zelinska, 2017). The protesters who resisted and stayed in Maidan Square were subjected to assault, kidnapping, illegal abductions, and loss of work, and additionally, the government formed new laws which restricted civil society and NGOs' right to protest (Zelinska, 2017). This further deteriorated the situation, ultimately weakening the social contract. After a lot of civilian and military casualties, Yanukovych and the opposition signed an agreement to put a halt to the political crisis, with the mediation of Russia and the EU (Chupryna, 2021). Soon after Yanukovych left the country; on 7 June 2014, the Ukrainian parliament appointed Petro Poroshenko as the new President, however, the situation only worsened because the Russians in Crimea felt threatened that Russia's influence might disappear in the region (Chupryna, 2021).

In the meantime, Russian officials and media channels initiated an unparalleled propaganda campaign portraying that the protests were a result of United States involvement, while there was no concrete evidence to back the claims (Nakashima, 2017). Russia took advantage of Ukraine's poor situation, particularly in Crimea, where the majority (more than half of the population) were widely believed to be pro-Russian (Iasiello, 2017). To gain support for Russia's actions in Crimea and increase the necessity for Russian intervention to protect indigenous Russian speakers, the country used pro-Russian news sources by mimicking the voices of Ukrainian and Western officials to shape public opinion (Iasiello, 2017). These news sources would

communicate wrong information and spread propaganda about the events taking place in Crimea – particularly blaming the West while refuting Russia's enrolment in the crisis (Iasiello, 2017).

One crucial lesson ingrained in the Russian leadership is how rapidly the data is disseminated with the help of the Internet by news agencies and personal blogs. President Vladimir Putin thus provided financial support to media experts, pro-Russian bloggers, journalists, and other high-profile individuals to form various identities on the web, create blogs on different accounts, and make comments to gain maximum support for Russian intervention (Iasiello, 2017). In some instances, these media experts would circulate images to pro-Russians which portrayed a huge number of immigrants crossing Ukraine's border and moving into Russia, while the reality was unlike; the images were of people who used to travel between Ukraine and Poland every day (Snegovaya, 2015).

Given a lot of confusion and unrest in the political sphere, the parliament of Ukraine was divided into portions: some were in favour of joining the EU, others wanted to remain autonomous, and the majority were in favour of joining Russia (Jaitner & Mattsson, 2015). In an all-night meeting which lasted till the early morning of 22nd February 2014, Putin along with other high officials of Russia decided to occupy Crimea. A well-known Russian group called "The Night Wolves" would support pro-Russians, sparking demonstrations against the Ukrainian government, and ultimately leading to the blockade of the Crimean parliament (Ketenci & Nas, 2021).

On February 27, 2014, the special forces of Russia, who were widely known as 'Little Green Men' (with no badges or signs on uniforms), took control of the government offices while raising the Russian flag on top of buildings (Bouwmeester, 2021). To avoid any uprising, the Russian troops disrupted the communication system by cutting off the telephone lines (Bouwmeester, 2021). Later, the Russian troops were also joined by the 'Wagner' which is a private security group – in addition, one of the units of GRU termed 'Fancy Bear' created numerous accounts on Facebook and started posting stuff that would generate negative perceptions about the West and Ukrainian officials. The Russian military exercises continued until 16 March 2014 when polls were held in Crimea – a majority of the Crimean population opted to be separated from Ukraine, which was possibly due to the pro-Russian popular narrative, and finally, on 18th March, a deal was signed in Moscow between the Crimean and Russian leadership to integrate the two regions (Bouwmeester, 2021).

Russian President Vladimir Putin initially denied any involvement in the Crimean crisis, however, following the integration deal, things started to open up, and the most compelling part of the invasion was that Russia kept the Western powers at bay, thus, influencing the parliament of Ukraine and remaining successful in convincing them to

integrate with Russia. The seizure of Crimea represents information as an effective tool of war – despite the presence of Ukraine forces in Crimea, Russia was able to shock them. The effectiveness of the information operations can be understood from two things: first, the fact that just in a matter of weeks, without using any sophisticated weapons, Russians were able to bury the will of Ukrainian forces and about 190 units present in the Crimean Peninsula surrendered. Second, the people were convinced enough that during the referendum on 16 March, the majority of the population voted for integration with Russia, which gave the state legitimacy to govern, hence portraying the move as democratic (Bouwmeester, 2021).

Information Warfare in the Ukraine War

Following the footsteps of the Georgian crisis and the Crimean invasion, Russia started to endorse its narrative in Ukraine due to the fear that it might join NATO. The Russian-backed network of trolls called Internet Research Agency (IRA), a key player in the 2016 US presidential elections, was once again assigned a task to disseminate fake news and run propaganda campaigns during the war. Earlier before the full-scale invasion by Russia, the government, military and financial websites of Ukraine were met with two distributed denial-of-service (DDoS) attacks, designed to overwhelm websites with false information requests. A destructive computer virus was found on numerous computers in Ukraine. Just as Russia's full-scale invasion of Ukraine began, several Russian-language accounts on X (formerly Twitter) started spreading fake news about the events (Muscat & Siebert, 2022).

Soon when Ukrainian officials realised this, they started countermeasures vis-a-vis Russian information offensives, with the support of Western tech firms including Planet Labs, Palantir Technologies, BlackSky Technology, and Maxar Technologies. The government officials and state citizens on both sides utilized multiple social media platforms such as TikTok, X, Facebook, Telegram and YouTube, to spread disinformation – video content across TikTok tagged with #Ukraine and #Russia garnered 8.5 billion and 37.2 billion views respectively in the first week of the war. Since most of the US-based social media platforms and websites are restricted in Russia, citizens use Virtual Private Networks (VPN) to access them. Apart from that, the majority of the Russian population uses Vkontakte (VK), Yandex, and Telegram for online communication, and these practices are still ongoing (Perez & Nair, 2022).

Furthermore, the role of deepfakes and bots proved phenomenal throughout the war, particularly on Twitter. Both Putin and Zelensky were repeatedly portrayed giving remarks about the conflict. Deepfakes of President Putin and Zelensky widely circulated over X calling on their forces to lay down arms, which received 50,000 and 120,000 views respectively (Perez & Nair, 2022).

In addition, British journalist Catherine Belton reported that in January 2023, President Putin's administration called on Russian political strategists to devise a social media strategy against President Zelensky of Ukraine, to portray him as weak, agitated, and self-centred. The meeting was followed by thousands of fabricated articles and social media posts distributed in Ukraine and across Europe. One fabricated Facebook post claimed that the family members of a deceased Ukrainian soldier had not obtained any support from the state, which received two million above views. Another fake post on Telegram claimed that the officials in Kyiv intended to "fight till the last Ukrainian is dead." These efforts which Moscow labelled as "information-psychological operations," were aimed at discrediting Kyiv's political leadership, demoralizing its troops, and dividing the Ukrainian population (Belton, 2024).

To create a rift among the political leadership of Ukraine, one Facebook post was planted by the Kremlin strategists claiming that General Valerii Zaluzhny "might be Ukraine's next president," which was viewed by 4.3 million people. Consequently, Zelensky's popularity decreased, as Kyiv polls showed that trust in Zelensky declined from 81% in July 2022 to 69% in February 2024 (Belton, 2024). Russia's efforts did make an impact; however, it fell short of meeting expectations because Ukraine had enough time to familiarize itself with the Russian information confrontation strategy since the annexation of Crimea. Moreover, Ukraine had and still has the support of Western technology firms, something which was miscalculated by the Russian leadership. Unlike in the past two events, this time both sides used social media extensively to depict their side of view and strengthen opposing perceptions about the war, entailing its motives, consequences, and prolongation.

Conclusion

Information warfare has evolved to a greater extent with the introduction of new technologies particularly in cyberspace where viruses such as trojan horses can be used to extract enemy data. Countries that are technologically more advanced have greater chances of being affected by information warfare techniques. In such a military-advanced world, for states to resort to hard means is more of suicidal, specifically in the case of nuclear weapons states – using conventional forces is no longer a viable option given the high cost of war. In such a scenario, states rely on non-conventional methods to wage a war. In this context, Russians have paced out other nations given their continued development in this domain. Russian information offensives work on a key principle of 'divide and conquer," by creating chaos and confusion among the enemy leadership and population. As famously quoted by Sun Tzu in The Art of War: "A confused enemy is much easier to defeat" – here, Russia has made a significant development and continues to use information warfare methods to achieve an upper hand over the enemy. Lessons that Russia learned from the Georgian conflict were

applied in the annexation of Crimea. Initially, when the Russian authorities tasked GRU firefighters to create chaos and spread disinformation in Crimea, made it much easier for the country to take over. Moreover, by making use of cyberattacks at the right time, Russia was successful in disrupting the communication lines of the Ukrainian authorities in 2014. While Russia did not gain much from the war in Ukraine, its experiences entail many lessons for military strategists. In a nutshell, the Russian information and psychological operations in Georgia, Crimea, and Ukraine provide a profound consideration of the conduct of information warfare – given the use of sophisticated techniques and the coordination between political, military, and media units. It provides insights into the changing nature of warfare and leaves signs for future conflicts.

References

A 5-Minute Guide to Understanding Ukraine's Euromaidan Protests. (n.d.). Retrieved February 11, 2025, from https://www.opensocietyfoundations.org/explainers/understanding-ukraines-euromaidan-protests

Abbott, D. (2010). The Handbook of Fifth-Generation Warfare. Ann Arbor: Nimble Books, 20.

Allegri, R. (2023). Russian Full Spectrum Conflicts and information warfare as Complex Adaptive Systems: The 2014 Crimean case study. Comparative Strategy, 42(4), 528–555. https://doi.org/10.1080/01495933.2023.2219193

Belton, C. (2024). 'Kremlin runs disinformation campaign to undermine Zelensky, documents show'. The Washington Post. https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/

Bouwmeester, C. H. (2021a). The art of deception revisited (part 2): The unexpected annexation of Crimea in 2014. https://militairespectator.nl/artikelen/art-deception-revisited-part-2-unexpected-annexation-crimea-2014

Chupryna, O. (2021). Ukraine's Euromaidan Revolution: A Final Breakaway from Russia. Geopolitical Monitor, 25. https://www.geopoliticalmonitor.com/ukraines-euromaidan-revolution-a-final-breakaway-from-russia/

Cohen, A., & Hamilton, R. E. (2011). The Russian military and the Georgia war: Lessons and implications. Strategic Studies Institute. https://www.files.ethz.ch/isn/130048/pub1069.pdf

Federation, R. (2000). Information security doctrine of the Russian Federation. United Nations International Telecommunications Union (ITU) Archive. https://base.garant.ru/182535/#friends.

Gavin Wilde and Justin Sherman, "No water's edge:... - Google Scholar. (n.d.). Retrieved February 11, 2025, from https://carnegieendowment.org/research/2023/01/no-waters-edge-russias-information-war-and-regime-security?lang=en

Golubchikov, O. (2017). From a sports mega-event to a regional mega-project: The Sochi winter Olympics and the return of geography in state development priorities. International Journal of Sport Policy and Politics, 9(2), 237–255. https://doi.org/10.1080/19406940.2016.1272620

Iasiello, E. J. (2017). Russia's improved information operations: From Georgia to Crimea. The US Army War College Quarterly: Parameters, 47(2), 7. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2931&context=parameters

Jaitner, M., & Mattsson, P. A. (2015). Russian information warfare of 2014. 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 39–52. https://ieeexplore.ieee.org/abstract/document/7158467/

Jones, A., Kovacich, G. L., & Luzwick, P. G. (2002). Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1. Information Systems Security, 11(4), 9–20. https://doi.org/10.1201/1086/43322.11.4.20020901/38841.3

Ketenci, A., & Nas, Ç. (2021). A Constructivist Perspective: Russia's Politics on Ukraine and Annexation of Crimea (2014). Bilge Strateji, 12(22), 53–88. https://dergipark.org.tr/en/download/article-file/2079844

Khan, K. (2012). Understanding information warfare and its relevance to Pakistan. Strategic Studies, 32, 138–159. https://issi.org.pk/wp-content/uploads/2014/06/1379480610_58047454.pdf

Konończuk, W. (2013). Ukraine withdraws from signing the Association Agreement in Vilnius: The motives and implications. Retrieved from Centre For Eastern Studies: https://www.osw.waw.pl/en/publikacje/analyses/2013-11-27/ukraine-withdraws-signing-association-agreement-vilnius-motives-and

Levine, Y. (2008). The CNN effect: Georgia schools Russia in Information warfare. Russia, August, 13. https://exiledonline.com/the-cnn-effect-georgia-schools-russia-in-information-warfare/

Muscat, S., & Siebert, Z. (2022a). Laptop generals and bot armies: The digital front of Russia's Ukraine war. Heinrich Böll Stiftung, Brussels Office, European Union, 1. https://eu.boell.org/en/2022/03/01/laptop-generals-and-bot-armies-digital-front-russias-ukraine-war

Nakashima, E. (2017). Inside a Russian disinformation campaign in Ukraine in 2014. Washington Post, 25. https://www.washingtonpost.com/world/national-

security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html

No Water's Edge: Russia's Information War and Regime Security. (n.d.). Carnegie Endowment for International Peace. Retrieved February 11, 2025, from https://carnegieendowment.org/research/2023/01/no-waters-edge-russias-information-war-and-regime-security?lang=en

Oltsik, J. (2009). Russian cyber attack on georgia: Lessons learned? Network World, 17. https://www.csoonline.com/article/547308/cisco-subnet-russian-cyber-attack-on-georgia-lessons-learned.html

Perez, C., & Nair, A. (2022). Information warfare in Russia's war in Ukraine. Foreign Policy, 22. https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/

Pietkiewicz, M. (2018). The military doctrine of the Russian Federation. Polish Political Science Yearbook, 47(3), 505–520. https://www.researchgate.net/publication/330109811_The_Military_Doctrine_of_the_Russian_Federation

Porkoláb, I. (2024). A Geraszimov-doktrína folytatása: Az orosz–ukrán háború tapasztalatai a stratégia tükrében. Honvédségi Szemle–Hungarian Defence Review, 152(5), 18–27. DOI: https://doi.org/10.35926/HSZ.2024.5.1

Russian Invasion of Ukraine: How Putin lost in 10 days. (n.d.). Imperial War Museums. Retrieved February 11, 2025, from https://www.iwm.org.uk/history/how-Putin-lost-in-10-days

Shah, H. J., & Ehsan, M. (2022). Hybrid Warfare: Emerging Challenges for Pakistan. Journal of Contemporary Studies, 11(2), 69–85. https://jcs.ndu.edu.pk/site/article/view/234

Snegovaya, M. (2015). Putin's information warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare', Russia Report, 1, 133–135. https://www.files.ethz.ch/isn/193932/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf

Stephenson, P. (1999). Information Warfare, or, Help! The Sky Is Falling! Information Systems Security, 8(1), 6–10. https://doi.org/10.1201/1086/43304.8.1.19990301/31046.2

Thomas, T. L., Blank, S., & Weitz, R. (2010). Russian information warfare theory: The consequences of August 2008. JSTOR. https://www.jstor.org/stable/pdf/resrep12110.8.pdf

Tzu, S. (2007). The art of war (trans. Lionel Giles). Forgotten Books.

Understanding Ukraine's Euromaidan Protests—Open Society Foundations. (n.d.). Retrieved February 11, 2025, from https://www.opensocietyfoundations.org/explainers/understanding-ukraines-euromaidan-protests

Wilde, G., & Sherman, J. (2023). No water's edge: Russia's information war and regime security. https://policycommons.net/artifacts/3363665/no-waters-edge/4162331/

Zelinska, O. (2017). Ukrainian Euromaidan protest: Dynamics, causes, and aftermath. Sociology Compass, 11(9), e12502. https://doi.org/10.1111/soc4.12502

Murakhovsky told what the new Russian military doctrine can surprise with "Mental Wars and Non-Nuclear Deterrence" (2021, April 3). https://www.mk.ru/politics/2021/04/03/murakhovskiy-rasskazal-chem-mozhet-udivit-novaya-rossiyskaya-voennaya-doktrina.html