Social Media as a Strategic Advantage During Cyberwarfare: A Systematic Literature Review

Errol Baloyi[1], Oyena Mahlasela[1], Nokuthaba Siphambili[1] and Mayan Stegmann[2]
[1]CSIR, Pretoria, South Africa
[2]Nclose, Cape Town, South Africa

EBaloyi2@csir.co.za
OMahlasela@csir.co.za
NSiphambili@csir.co.za
Mayan@Nclose.com

Abstract: In recent years, cyberspace has been shaped by a rapid and transformative technological evolution, which ushered in an era characterised by unparalleled connectivity and innovation. However, this remarkable progress has brought a concerning surge in cyberattacks that have fundamentally altered cyberspace dynamics and refined the nature of contemporary warfare. This refinement was vividly illustrated in the recent Russia-Ukraine conflict, where cyberspace played a pivotal role, blurring the traditional boundaries of conflict in the cyber age. As a result, this study used secondary data to examine how various social media platforms such as Twitter, Facebook, TikTok, and Telegram were used as a strategic advantage during the conflict. The findings disclosed that Russia employed offensive propaganda against Ukraine, while Ukraine adopted a defensive stance, effectively countering the narrative through an active online presence. Moreover, this study underscored the substantial role of social media in warfare and its continued significance in future conflicts. Furthermore, this study provided recommendations for nations to better prepare for such conflicts. The recommendations provide valuable insights to assist decision-makers and policymakers in enhancing cybersecurity awareness and practices within their respective countries.

Keywords: Cyberattacks, Cyberspace, Cybersecurity, Russia-Ukraine, Warfare, Social media

1. Introduction

Since the early 1990s, cyberwarfare has been recognized by its advocates as a groundbreaking military revolution and a highly effective tool in combat, but these was primarily theoretical until the recent Ukraine-Russia conflict where cyberspace was utilized during the conflict (Schulze and Kerttunen, 2023). Even so, several countries have already made notable progress in terms of preparedness, following the Warsaw Summit 2016, where the North Atlantic Treaty Organization (NATO) declared cyberspace as a battlefield, which lead to member countries establishing their respective cyber commands (Smeets, 2023). However, Russia has always demonstrated remarkable proficiency as a cyber power worldwide. Instances of their cyber activities trace back to Moonlight Maze attacks on the United States Department of Defence in the 1990s and suspected involvement in cyberattacks against various targets, including the Estonian government, media, and financial sectors in 2007, Georgian government sites in 2008, Kirgizstan Internet Service Provider attacks in 2009, and Ukrainian government, military, and critical infrastructure attacks in 2014 (Priyono, 2022).

The tensions between Russia and Ukraine have witnessed a significant escalation since 2014, notably characterised by the annexation of Crimea following a contentious local referendum. These tensions have continued to intensify over time, resulting in substantial cyberattacks, particularly targeting Ukrainian power utilities. Moreover, in December 2015 and 2016, over 225,000 individuals in Ukraine experienced power outages due to cyberattacks, with Kyiv also facing similar disruptions (Priyono, 2022). Furthermore, in June 2017, the global impact of the NotPetya cyberattack, attributed to Russia, led to considerable financial losses. After Russia invaded Ukraine on February 24, 2022, cyber warfare played a pivotal role in shaping and influencing international events. This encompassed attacks on communication systems, government websites, border control stations, and Ukraine's digital infrastructure (Przetacznik and Tarpova, 2022). Additionally, Russia employed various tactics, including the manipulation of information through social media, fabricating American military profiles on Twitter to exploit anti-government sentiments and sway populations toward pro-Russian stances (Littell and Starck, 2023; Weinberg, Dawson and Edwards 2023).

2. Methodology

A systematic literature review was conducted to synthesise existing literature on cyberwarfare to understand the use of social media as a strategic advantage during cyberwarfare. The search protocol followed was the Preferred Reporting Items for the Systematic and Meta-analysis (PRISMA) framework (Sarkis-Onofre et al., 2021).

2.1 Identification

Relevant publications were identified through the search terms (*"cyber warfare", "cyberattacks", "cyberspace", "cybersecurity", and "social media").* The search term was then applied to different scholarly databases such as IEEE Digital Library, Scopus, Science Direct and Google Scholar search engine.

2.2 Screening

The publications identified from the scholarly databases were screened, where abstracts were read, and irrelevant studies were eliminated. This was done through the selection criteria applied to get relevant publications—the selection criteria comprised of the inclusion and exclusion criteria as shown in Table 1.

Table 1: Selection criteria exclusion and inclusion

Exclusion	
EC1	Duplicates of the same article retrieved from different database
EC2	Articles that were irrelevant to the study
EC3	Articles that were not written in English
Inclusion	
IC1	Articles that were relevant to cyber warfare and used social media as the strategy
IC2	Articles published between 2022 and 2023

2.3 Eligibility

After applying exclusion and inclusion criteria (n=57), publications were left for eligibility assessment. The eligibility assessment involved reading the whole research article, and the studies found illegible were excluded.

2.4 Included

The publications found legible and considered in the full review are (n=19).

3. Results

Warfare is not new; it has always been a persistent aspect of human history, spanning various conflicts like the Battle of Lepanto, the Napoleonic Wars, the World Wars, The Vietnam War, and so forth (Desai and Manabat, 2022). However, what has evolved is the methods employed in warfare, progressing from primitive wooden spears and rudimentary weaponry to advanced machinery. In the contemporary era, warfare has incorporated a cyber dimension, for instance, using social media to disseminate disinformation during warfare. According to Henkhaus (2022) in the past, disseminating false or misleading content, or even accurate information, required the resources of a state or a powerful actor. However, in the contemporary landscape, anyone can create a TikTok video and instantly share it with a global audience.

3.1 Misinformation and Propaganda

Presently, social media has emerged as the primary platform for disseminating misinformation and conducting propaganda campaigns, often leveraging fabricated content such as false photos, and manipulated videos (Konstankevych et al., 2022). The strategic use of disinformation as a weapon of war seeks to impede international relations, erode public trust in leaders and institutions, and tarnish opposing political ideologies (Morejón-Llamas et al., 2022). Notably, Russia employed this tactic during the conflict. This is because the expansive reach of social media not only enables the instant dissemination of false information but also serves as a powerful tool for influencing public opinion. According to Konstankevych et al. (2022) disinformation model, there are four primary components of disinformation: denial of truth and facts, distortion and twisting of facts, distraction and blame, and Intimidation, causing panic and anxiety. Consequently, this study attempts to align its results to that model to better highlight how social media was used as a strategic advantage during the conflict.

The denial of truth and facts often involves the manipulation of information. Astuti, Attaymini, and Dewi (2022) noted that this manipulation can be characterised as propaganda when used to achieve specific goals. A study conducted by Shultz (2023) is one of the many studies that delve into Russian propaganda, focusing on the top ten topics discussed by Russian government social media accounts. The study found that the primary focus was on the 77th meeting of the United Nations (UN) General Assembly that took place on September 13, 2022. Many tweets from those Russian government accounts engaged in extensive discussions about multilateral relations

and U.N. issues, aiming to depict Russia as a peacekeeping and prominent international player. This communication strategy was recurrently employed by Russian government accounts despite international condemnation of Russia's aggressive actions against Ukraine by the UN.

Following the invasion of Ukraine, Pierri et al. (2023) observed a significant decrease in the prevalence of Russian propaganda. This decline was attributed to the implementation of new policies on various platforms, European regulations targeting Russian propaganda, and Russia's ban on online social networks. However, Górka (2022) cautioned against underestimating Russian influence despite potential setbacks in the information war in Ukraine and the West. In line with this, Geissler et al. (2023) asserted that Russian propaganda has evolved over time, employing new tactics that likely involve an increased use of bots. As defined by Ferrara et al. (2016), social media bots are computer algorithms designed to generate content automatically and engage with humans on social media platforms, aiming to emulate and potentially alter their behaviour.

As social media platforms continue to play an increasingly significant role in people's lives, the influence of bots in shaping individual opinions and public sentiment grows. Particularly when social media becomes a tool for advancing national interests and political propaganda, it can be harnessed to challenge societal and international norms (Shen et al., 2023). Bots offer the capacity to generate many software-controlled social media profiles at a low cost. Even though bots tend to post and receive fewer retweets than human users within social media networks, they still manage to garner more attention than human accounts. Consequently, they can effectively disseminate content that might not gain traction otherwise. A study by Geissler et al. (2023) affirmed the existence of Russian-coordinated campaigns utilising bots, with 20.28% of the information spreaders classified as bots. Many of these bots were created at the outset of the invasion. The study also indicated that bots played an amplifying role in the early dissemination of information. Notably, India, South Africa, and the United States emerged as primary targets for these bots.

Shen et al. (2023) study also supports the findings with a study that examined the popularity of the top 20 hashtags in bot and non-bot tweets, revealing that a significant proportion of social media bots engaged in online conversations during the Russia-Ukraine conflict. Intriguingly, the data showed that tweets from Russian-side bots received a higher average number of retweets, likes, and comments compared to those from the Ukrainian side. Surprisingly, even though Russia was a key participant in the conflict, very few bot accounts identified themselves as being from Russia. Kuźmiński's (2022) further confirmed the presence of Russian propaganda, particularly on video-sharing platforms. Some of the propaganda efforts included the exclusive use of the term "special operation" in Russian narratives, sidestepping accurate descriptions like "war" or "full-scale invasion".

To justify their invasion, the Russian government employed distraction and blame tactics. For instance, they propagated narratives suggesting that Ukraine was a breeding ground for Nazism and had a close relationship with the United States. Additionally, Russia accused Ukraine of stealing gas from "Gazprom" without payment, all to justify and conceal the crimes committed by the Russian military in Ukraine. Russian propaganda sought to distort the course of the war among its citizens and portrayed Ukrainians in a negative light (Konstankevych et al., 2022). Furthermore, the Russian government employed intimidation tactics, causing panic and anxiety among the Ukrainian people. They spread stories suggesting that after the invasion, Ukrainian President Volodymyr Zelenskyy had fled abroad (Astuti et al., 2022). They also alleged that the Ukrainian Armed Forces were sending untrained soldiers into battle and that there was a food shortage in Ukraine (Konstankevych et al., 2022). In a particularly damaging move, a video was circulated that purported to show Ukraine's President surrendering to Russia (Kuźmiński, 2022). Notably, some of these false narratives and videos were shared by verified accounts, adding an additional layer of credibility to the disinformation (Haq et al., 2022).

3.2 Information Dissemination and Mobilizing Public Backing

In the period of transitioning from a looming threat of war to the actual invasion by Russia, Ukrainian leaders, specifically President Zelenskyy, adeptly managed the global demand for information. This skilful handling of information was pivotal to Ukraine's success in information warfare. President Zelenskyy actively engaged in various information campaigns to inform and bolster the morale of the Ukrainian populace. A noteworthy moment occurred in April 2022, approximately six weeks into Russia's invasion of Ukraine, when President Volodymyr Zelensky made a plea at the 2022 Grammy Music Awards, urging the audience to share Ukraine's story on social media, encapsulated by the phrase "Fill the silence" (Serafin, 2022). Subsequent research, exemplified by Sazzed's (2022) study, which involved the analysis of over 80,000 tweets from seven different countries, each representing diverse demographic groups expressing their sentiments and opinions about the conflict, consistently favoured Ukraine, with a prevalent negative sentiment towards the war.

This was a very strategic move by Ukraine, recognising their limitations in cyber capabilities when compared to Russia, prompting them to leverage the power of President Zelensky's speeches and video clips as a formidable means of disseminating information and seeking international assistance. This approach exploited the sympathy and sense of responsibility within the Western world and Ukraine's natural allies (Munk & Ahmad, 2022). Zelensky's omnipresence on various platforms, including TikTok, where "I'm a Zelensky stan" amassed 7.3 million views, and the curiosity surrounding his war attire on Twitter illustrated how he became a source of inspiration. Furthermore, he provided daily updates to the Ukrainian people about the war's status and the necessity of resilience. This exemplified a twenty-first-century form of warfare where information dissemination might outshine physical battlefield actions (Serafin, 2022). However, it's essential to underline that while cyber operations can amplify military efforts, they are most effective when integrated with conventional warfare strategies (Fedotenko, 2023).

Ukraine's Minister for Digital Transformation, Mykhailo Fedorov, also employed a multifaceted strategy to counter Russia's actions. One of his tactics involved reaching out to major tech companies like Meta and Google through Twitter, urging them to block Russian access to their platforms and services. Additionally, Fedorov personally contacted Elon Musk to request assistance in deploying Starlink satellite internet systems to enhance communication capabilities across Ukraine. Furthermore, in the early stages of the invasion, Fedorov took an unprecedented step by issuing a "call to arms" for a civilian cyber army to bolster Ukraine's defence. This call to action was conducted on the encrypted messaging app Telegram. It's worth noting that Telegram served a unique role in this context; while Facebook was limited by legal constraints, Telegram became a hub for activities that fell into the realm of cyberwarfare. Specifically, Telegram groups were utilised to coordinate and organise cyberattacks on Russian websites and services (Ronzhyn, Cardenal, and Batlle, 2023; Serafin, 2022).

According to Ronzhyn et al. (2023), fundraising also emerged as the most prevalent activity on social media during the conflict. Their study analysed Facebook profiles engaged in fundraising and found that while most profiles existed before the onset of the war, they experienced significant growth during the conflict. Similarly, Pohl et al. (2022) delved into analysing 8.7 million original tweets generated by 2.3 million unique user accounts between February 17 and March 3, 2022. Their findings indicated numerous accounts seemingly took advantage of the Ukrainian government's call for cryptocurrency donations. This highlights the dual nature of social media during conflict. While it can be a platform for noble actions like fundraising, there is also a tendency for exploitation. As a result, it is imperative to consider the following recommendations to address these issues.

4. Recommendations

The use of social media platforms to disseminate disinformation, propaganda, and misinformation has the power to shape public perceptions, influence political dynamics, and even impact national security (OECD, 2022). This section delves into recommendations that can empower policymakers, organisations, and individuals to combat the adverse effects of these information warfare campaigns. The reality is that, during future conflicts, it will be crucial to prepare nation-states to employ comprehensive legal frameworks. While respecting free speech, enhancing media literacy, and moderating content in the private sector. Individual users should become vigilant while informed about the conflict. As a result, by providing these recommendations, the authors aim to foster a more informed and resilient society that can better navigate the complex landscape of information warfare in a time of conflict.

4.1 The Role of the Policymaker at a Nation-State Level

During future conflicts, at a nation-state level, policymakers will likely find themselves at the forefront of the battle against disinformation and propaganda. Therefore, this study recommends the development of a framework that will be responsible for addressing the emergence of disinformation and propaganda whilst considering the rights of citizens. The European Parliament briefly highlighted this responsibility by stating that every government has a duty to uphold the Universal Declaration of Human Rights (UDHR), which Article 19 of the UDHR states that: ‘Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers (Colomina, Margalef, and Youngs 2021). Similarly, South Africa and other nations have such regulations. Hence, the goal is to strike a delicate balance by developing and enforcing a new framework that addresses disinformation while upholding fundamental principles of free speech. This framework must provide clear guidelines to distinguish between protected free expression and harmful disinformation, ensuring the latter is appropriately addressed without infringing upon the rights of citizens.

Furthermore, Levush (2019) proposes that policymakers should establish specialised government agencies or units with a mandate to monitor and detect disinformation campaigns. Hook and Verdeja (2022) support this notion by stating that these agencies should be equipped with advanced analytics tools to identify patterns and tactics employed by malicious actors, enabling swift detection and response to emerging disinformation threats. The United Kingdom's (UK) government communication service has already made headway by developing the RESIST 2 Counter Disinformation Toolkit, which is responsible for detecting and responding to online disinformation and fake news campaigns (Pamment, 2021). Therefore, we also recommend that policymakers must also invest in technology and expertise to detect and combat automated bots and troll accounts, which are frequently used to amplify disinformation. Additionally, collaborative and information-sharing partnerships with other nations and international organisations should be prioritized for tackling cross-border disinformation threats, as the interconnected nature of social media necessitates global cooperation and collective responses.

4.2 Countering Disinformation in the Private Sector

According to the UN, the private sector has a non-binding responsibility to respect human rights (UN, 2016). As a result, the largest social media platforms are increasingly implementing policies and functions to protect the human rights of their users and counter the spread of disinformation (Colomina et al., 2021). Concurrently, organisations must invest in media literacy training for their employees, especially those managing social media accounts or interacting with the public (Van Audenhove et al., 2018). Furthermore, it is essential to implement content moderation and reporting mechanisms to promptly remove or label false information on their social media accounts and platforms. Additionally, the private sector organizations should develop a crisis communication plan that outlines protocols for responding to disinformation campaigns targeting their organisation and coordinate response. Furthermore, collaboration with fact-checking organisations, governmental agencies, and other organisations for information sharing and resource pooling is also recommended. Transparency in communication is essential for building trust with the audience.

4.3 The Role of the Individual as an End User of Social Media

According to Colomina et al. (2021), individuals as the end user of social media, play a critical role in countering disinformation online. Therefore, development of media literacy is a necessary first step in being able to identify misinformation, disinformation, and propaganda. As a result, we recommend enrolment of online courses and resources to enhance individual’s media literacy skills. Furthermore, fact-checking is another essential practice, where individuals verify the information before sharing it by using reputable fact-checking websites and avoiding disseminating unverified information (Apuke et al., 2022). Likewise, employing critical thinking, questioning the source of information, and maintaining scepticism toward sensational or biased content are good practices. Moreover, individuals should verify the legitimacy of websites by examining URLs and domains while being cautious of fake news sites that mimic credible news organisations. Thus, reporting false information through social media platform reporting tools is also encouraged. Importantly, individuals should refrain from engaging with, liking, or sharing disinformation and instead report it or inform others about its falsehood. Lastly, cultivating a diverse news feed by following various news sources and opinions helps individuals avoid living in echo chambers and gain a balanced perspective on current events.

5. Discussion

This study exhibited that social media has transcended its role as a mere communication tool and is now emerging as a potent weapon capable of shaping public opinion, influencing perceptions, and ultimately steering the course of events. This transformation was remarkably observed during the recent Russian-Ukraine conflict, where cyberspace played a crucial role from the outset. The incorporation of a cyber element in this conflict serves as a clear indication that the future of conflicts will likely involve cyber strategies, underscoring the necessity for nations to develop a resilient cyber posture. Furthermore, this study highlighted Russia’s offensive stance in the conflict, employing tactics such as disinformation and propaganda attacks against Ukraine to manipulate public opinion. The use of terms like "special operation" instead of "war" aimed at swaying public sentiment in favour of Russia. Despite these efforts, Ukraine successfully maintained a defensive position by maintaining a robust online presence. Leveraging social media, Ukraine also enlisted support from private companies and assembled an army of hackers to counteract Russia's formidable capabilities. Nevertheless, Russia persisted in its efforts. Despite facing restrictions from various companies, they resorted to the use of bots to perpetuate their propaganda and continue shaping public opinion against Ukraine. This underscores the

evolving landscape of warfare, where the role of social media is increasingly significant, necessitating strategic responses from nations to safeguard against such cyber threats.

6. Conclusion and Future Work

The spreading of propaganda and misinformation through social media during warfare represents a new dimension in warfare. Consequently, this study conducted a systematic literature review with a primary focus on the multifaceted role of social media in modern warfare, homing in on its specific utilisation during the Russia-Ukraine conflict. Furthermore, this study aimed to answer a critical research question: how was social media strategically leveraged during this conflict? This was because the Russia-Ukraine conflict served as a stark reminder that warfare extends beyond its conventional realms in the contemporary theatre of war. To comprehensively address the question, this study drew upon a diverse body of literature, synthesising valuable insights to dissect the intricate ways in which social media was and can continue to be employed as a strategic advantage in modern warfare. Beyond exploring its potential benefits, this study delved into the complex consequences of social media in warfare, shedding light on its multifaceted challenges. Furthermore, this study expanded its scope to examine countermeasures that can be employed to mitigate these effects, recognising the importance of a proactive approach in safeguarding national security interests.

The findings generated by this study hold significant implications for governments, law enforcement agencies, and national defence forces, by offering valuable insights to aid in their preparedness and strategic responses to the evolving dynamics of modern warfare. However, it is crucial to acknowledge that this study was constrained to secondary data. The authors recommend that for future work, it is crucial to broaden the scope and include primary data, as this will allow for a more comprehensive understanding of the pivotal role played by social media in the conflict and its ongoing influence on shaping future conflicts.

References

Apuke, O.D., Omar, B. and Tunca, E.A. (2023) "Effect of fake news awareness as an intervention strategy for motivating news verification behaviour among social media users in Nigeria: A quasi-experimental research", *Journal of Asian and African Studies*, Vol 58, No. 6, pp 888-903.

Astuti, Y.D., Attaymini, R. and Dewi, M.S. (2022) "Digital Media and War: Social Media as a propaganda tool for the Russia-Ukraine conflict in the post-truth era", *Proceedings of the Annual International Conference on Social Science and Humanities (AICOSH 2022*), pp 19–27. doi:10.2991/978-2-494069-87-9_4.

Colomina, C., Margalef, H.S., Youngs, R. and Jones, K. (2021) *The impact of disinformation on democratic processes and human rights in the world*, Brussels: European Parliament.

Desai, D. and Manabat, H. (2022) "CyberWarfare: The Past, The Present and the foreseeable future", CPSC - 558 Advanced Computer Networking [Preprint].

Fedotenko, K. (2023) "Cyber warfare as part of information warfare of Russia against Ukraine since the beginning of the 2022 Russian invasion", *Věda a perspektivy,* Vol 8, No. 27, pp 351-357.

Ferrara, E., Varol, O., Davis, C., Menczer, F. and Flammini, A. (2016) "The rise of social bots", *Communications of the ACM*, Vol 59, No. 7, pp 96–104.

Geissler, D., Bär, D., Pröllochs, N. and Feuerriegel, S. (2023)" Russian propaganda on social media during the 2022 invasion of Ukraine", EPJ *Data Science*, Vol *12, No.* 1, pp 35.

Giannaris, P.S., Karamanoli, V., Agathocleous, A., Ilias, I. and Doukas, N. (2022) "Text similarity study for Twitter-based news on Russian-Ukraine cyber war", Paper read at 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp 1-8, Athens, Greece, December.

Górka, M. (2022) "A definitional framework for cyber warfare. The Ukrainian aspect", *Polish Political Science Yearbook*, Vol 51, No .1, pp 1–14.

HHS Cybersecurity Program, (2022). The Russia-Ukraine Cyber Conflict and Potential Threats to the US Health Sector, [online], Administration for Strategic Preparedness and Response (ASPR), https://www.aha.org/system/files/media/file/2022/06/HHS-TLP-White-The-Russia-Ukraine-Cyber-Conflict-and-Potential-THreats-to-the-US-Health-Sector-3-1-22.pdf.

Haq, E.U., Tyson, G., Braud, T. and Hui, P. (2022) "Weaponising social media for information divide and warfare", *In Proceedings of the 33rd ACM Conference on Hypertext and Social Media*, Barcelona, Spain, July, pp 259-262.

Henkhaus, L. (2022) "The role of the internet in Ukraine's Information War", [online], Texas A&M Today, https://today.tamu.edu/2022/03/14/the-role-of-the-internet-in-ukraines-information-war/.

Levush, R. (2019) Government Responses to Disinformation on Social Media Platforms: Argentina, Australia, Canada, China, Denmark, Egypt, European Union, France, Germany, India, Israel, Mexico, Russian Federation, Sweden, United Arab Emirates, United Kingdom. Publication, pp 1–177.

Littell, J. and Starck, N. (2023) "Russian influence operations during the invasion of Ukraine", *International Conference on Cyber Warfare and Security*, Vol 18, No. 1, pp 209–217.

Konstankevych I., Kostusiak N., Shulska N., Stanislav O., Yelova T., and Kauza I. (2022) "Media Manipulation as a Tool of Information Warfare: Typology Signs, Language Markers, Fact Checking Methods", *Ad Alta,* Vol 12, No. 2, Spec. Iss. XXIX, pp 224–230.

Kuźmiński, A. (2022) "The methods of disinformation in the Russia-Ukraine war", *Rhetoric and Communications*, Vol 53, pp 167–171.

Morejón-Llamas, N., Martín-Ramallal, P. and Micaletto-Belda, J.P. (2022) Twitter content curation as an antidote to hybrid warfare during Russia's invasion of Ukraine, *Profesional de la información*, Vol *31, No.* 3.

Munk, T. and Ahmad, J., 2022. "I Need Ammunition, Not a Ride": The Ukrainian Cyber War". *Comunicação e sociedade*, Volu 42, pp 221-241.

OECDb., (2023) Principles of good practice for public communication responses, [online], OECD, https://www.oecd.org/gov/open-government/good-practice-principles-for-public-communication-responses-to-misinformation-and-disinformation.htm

Paavola, J., Helo, T., Jalonen, H., Sartonen, M. and Huhtinen, A.M. (2016) "Understanding the trolling phenomenon: The automated detection of bots and cyborgs in the social media", *Journal of Information Warfare*, Vol 15, No. 4, pp 100-111.

Pamment, J. (2021) "RESIST 2 Counter Disinformation Toolkit", Rep, UK Government Communication Service.

Priyono, U., 2022." Cyber Warfare as Part of Russia and Ukraine Conflict", *Jurnal Diplomasi Pertahanan, Vol* 8, No. 2, pp 44-59.

Pierri, F., Luceri, L., Jindal, N. and Ferrara, E. (2023), April. "Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine", In *Proceedings of the 15th ACM Web Science Conference 2023,* pp 65-74.

Pohl, J., Seiler, M.V., Assenmacher, D. and Grimme, C. (2022" A Twitter Streaming Dataset collected before and after the Onset of the War between Russia and Ukraine in 2022, *Available at SSRN 4066543*.

Przetacznik, J. and Tarpova, S. (2022) "Russia's war on Ukraine: Timeline of cyberattacks", *European Parliamentary Research Service (EPRS)*, pp 1-7.

Ronzhyn, A., Cardenal, A.S. and Batlle, A. (2023) "Collective action on Facebook and telegram during the Russia–Ukraine war", *European Conference on Social Media*, Vol 10, No.1, pp 223–230.

Sazzed, S. (2022) "The Dynamics of Ukraine-Russian Conflict through the Lens of Demographically Diverse Twitter Data", Paper read at 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 2022, pp 6018-6024.

Sarkis-Onofre, R., Catalá-López, F., Aromataris, E. and Lockwood, C. (2021) "How to properly use the PRISMA Statement". *Systematic Reviews,* Vol 10, No. 1, pp 1-3.

Serafin, T. (2022) "Ukraine's president Zelensky takes the Russia/Ukraine war viral", *Orbis*, Vol 66, No. 4, pp 460–476.

Shen, F., Zhang, E., Zhang, H., Ren, W., Jia, Q., & He, Y. (2023). Examining the differences between human and bot social media accounts: A case study of the Russia-Ukraine War. *First Monday*, *28*(2). https://doi.org/10.5210/fm.v28i2.12777

Schulze, M. and Kerttunen, M. (2023) "*Cyber operations in Russia's war against Ukraine: Uses, limitations, and lessons learned so far",* Berlin: Stiftung Wissenschaft und Politik (SWP).

Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T.H., Ding, K., Karami, M. and Liu, H. (2020) "Combating disinformation in a social media age", *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, Vol *10, No.* 6, pp 1385.

Shultz, B. (2023) "In the spotlight: The Russian government's use of official Twitter accounts to influence discussions about its war in Ukraine", In ACM International Workshop on Multimedia AI against Disinformation (MAD '23), Thessaloniki, Greece, June.

Smeets, M., (2023) "The challenges of military adaptation to the cyber domain: a case study of the Netherlands", *Small Wars & Insurgencies, Vol* 34, No. 7, pp 1343-1362.

Stănescu G. (2022) "Ukraine conflict: the challenge of informational war", *Social Sciences and Education Research Review*, Vol 9, No. 1, pp 146-148.

Talwar, S., Dhir, A., Singh, D., Virk, G.S. and Salo, J. (2020) "Sharing of fake news on social media: Application of the honeycomb framework and the third-person effect hypothesis", *Journal of Retailing and Consumer Services*, Vol 57, pp 102197.

UN., (2022) "Freedom of expression is key to countering disinformation", [online], UNHR, https://www.ohchr.org/en/stories/2022/11/freedom-expression-key-countering-disinformation.

Van Audenhove, L., Marien, I., Craffert, L. and Grove, W. (2018) South Africa's e-Skills Policy, From e-Skills to Media Literacy?, Paper read at *2018 IST-Africa Week Conference (IST-Africa)*, pp 1-11, Gaborone, Botswana, May.

Walker, S., Mercea, D. and Bastos, M. (2021) "Introduction to the disinformation landscape and the lockdown of Social Platforms", *Disinformation and Data Lockdown on Social Platforms*, pp 1–13.

Weinberg, D., Dawson, J. and Edwards, A. (2023) "How the Russian Influence Operation on Twitter Weaponized Military Narratives", *Proceedings of the 18th International Conference on Cyber Warfare and Security*, Vol 18, No. 1, pp 431-439.