REVIEW ARTICLE

ASIAN JOURNAL OF INTERDISCIPLINARY RESEARCH

Asian Research Association

DOI: 10.54392/ajir2541

Innovative Technologies in Information Warfare as a Means of Protecting National Interests of Ukraine and Georgia: A Literature Review

Leyla Derviş [a, *]

[a] Akdeniz University, Faculty of Letters, Department of Historical Sciences, Dumlupınar Bulvarı Kampüs, Pk.07058, Antalya, Turkey
* Corresponding author Email: leyladervis@akdeniz.edu.tr
DOI: https://doi.org/10.54392/ajir2541
Received: 26-06-2025; Revised: 11-09-2025; Accepted: 25-09-2025; Published: 09-10-2025

Abstract: Information wars are becoming increasingly important in modern conflicts, posing a serious threat to national security. Disinformation and cyber-attacks are an important element of the hybrid aggression of the Russian Federation, which Ukraine and Georgia have encountered. The article aims to identify the leading innovative technologies that contribute to the conduct of information warfare. The study is based on a content analysis of 34 scientific publications selected from Google Scholar, Scopus and Web of Science databases for the period from 1995 to the present. Key words such as "information warfare", "cyber-attacks", "Ukraine", "Georgia" and "national security" were used. Systematic and comparative methods were used to identify common and distinctive features in strategies to counter information threats. The results determined that the experience of Ukraine and Georgia offers valuable information about the dynamics of information warfare and its consequences for national security. Among the leading technologies used in hybrid warfare are artificial intelligence, social networks, deepfakes, bots, and cyber-attacks. Despite these challenges, both countries have taken steps to counter Russian influence and strengthen their resistance to disinformation. The experience of Ukraine and Georgia emphasizes the importance of countering information warfare in national security strategies. The findings showed that legislative, regulatory and technological measures are critical to mitigating the impact of disinformation campaigns and protecting democratic institutions.

Keywords: AI Technology, Cyber Secure, Georgia, Informational War, Russian Aggression, Ukraine

1. Introduction

Innovative technologies in information warfare have transcended their conventional role as mere tools for influencing mass society. They became pivotal to global politics and national security strategies (Panda & Giordano, 1999). Its pervasive influence on public opinion formation, information manipulation, and disinformation exposure reverberates across diverse regions. In this dynamic landscape, the experiences of nations embroiled under challenging periods of informational conflicts and wars, such as Ukraine and Georgia, offer invaluable insights into the intricate nature of information threats and the imperative to develop effective countermeasures. A comparative examination of the approaches to information security adopted by Ukraine and Georgia promises to unveil commonalities and distinctive features in their strategies for mitigating information threats.

Both Georgia and Ukraine have found themselves ensnared in a web of informational hybrid attacks orchestrated by the Russian Federation, primarily because of their unequivocal expressions of aspirations and strides toward European integration (Sashchyk & Rykhlik, 2022). The theoretical basis for the study is the work of Muradov (2022), Fedorchak (2024) and Cybulsky (2022), which contains several generalizations from previous studies and original conclusions about current events. When comparing their results with other works of scholars, specific problematic episodes that require further analysis are also identified. Meanwhile, Russia, propelled by deep-seated imperialist ideologies and a conviction of its historical superiority from the Middle Ages to the present (Mereniuk & Parshyn, 2024), employs various means to impede these endeavours. In such a milieu, information warfare transforms into an intellectual battleground where concepts, views, and strategies vie for supremacy, often manifested through succinct messages disseminated via news feeds and videos. Victory in this arena extends beyond the mere dominance of one narrative over another.

Information warfare encompassed various tactics to manipulate, distort, or control information to achieve strategic objectives. It involved using various media channels, cyber capabilities, psychological operations, and disinformation campaigns to influence target audiences' perceptions, attitudes, and behaviours (Church, 2000). With the emergence of cyberspace, information warfare perplexes military strategists as it unveils itself as a potent tool for widespread disruption (Chong, 2013). The study by Hutchinson (2002) delved into the essential principles necessary for comprehending the diverse range of activities associated with the phenomenon of information warfare. Contemporary researchers are deeply engaged in unravelling the intricate nature of the confrontations between Georgia and Russia and the subsequent hybrid warfare episodes involving Ukraine and Russia (Blănaru, 2024; Van Niekerk, 2024). As scholars meticulously dissect the strategies, tactics, and impacts of information warfare within these contexts, their overarching aim is to furnish invaluable insights into how nations navigate an ever-evolving landscape of security challenges within an increasingly interconnected and digitized world (Kernen & Sussex, 2012; Cybulsky, 2022). Examining these conflicts offers a multifaceted lens to comprehend the multifarious dimensions of contemporary security threats (Gamkrelidze, 2022). Amilakhvari and Baghaturia (2024) delved into Russia's aggressive rhetoric and expansionist policies, shedding light on how these factors contributed to information warfare dynamics. The study by Bartnicki et al. (2023) focused on the 2022 Russian-Ukrainian War and explored the role of information and information technologies in shaping the conflict. Horobets and Martyinov (2022) explored the relationship between political culture and identity politics in Ukraine. Horobets and Martyinov (2022) argued that a deeper understanding of these dynamics is essential for promoting social cohesion and political stability in Ukraine. The chapter by Kernen and Sussex (2012) comprehensively analyzed the Russian-Georgian War, including its information warfare dimensions. In addition, Deibert et al. (2012) examined the dynamics of information warfare during the 2008 Russia–Georgia War. Parshyn and Mereniuk (2023) showed historical "arguments" of Russian expansion plans.

Moreover, Gamkrelidze (2022) examined the role of information warfare in shaping Georgia's relationship with Russia. These studies underscored the importance of developing strategies for countering information warfare threats. However, a gap in these studies is the lack of a comparative analysis of modern innovative technologies for conducting information warfare.

Therefore, this article endeavours to undertake an in-depth analysis of the pivotal role played by information warfare in national security, drawing upon the experiences of Ukraine and Georgia as case studies.

This study analyses the leading technologies used to conduct information warfare in the context of national security protection in Georgia and Ukraine. Accordingly, the research questions are as follows:

1. What are the features of conducting information wars in these countries?

2. What are the leading technologies used?

3. Is the conduct of information warfare in Georgia different from its conduct on the territory of Ukraine?

2. Methodology

The work on the article was carried out in several stages, each involving specific research methods. Some results were obtained by applying the content analysis method of modern scientific literature, which made it possible to consider the current opinions of scholars on the peculiarities of Russian information wars against Georgia and Ukraine. For this purpose, the most relevant scientific works related to realizing the research goal were selected.

Specifically, an important method in the study was the use of the PRISMA approach. Specifically, at the initial stage, a list of keywords was used in the search for materials to characterize the issue of Russia's information wars against Georgia and Ukraine: "war," "information war," "Russian aggression," "Ukraine," "Georgia," "national security," "cyber technologies," "cyberattacks," and "artificial intelligence." The next stage involved a systematic search for scientific sources in the international scientific databases Google Scholar, Scopus, and Web of Science. The chronological range of scientific sources is set from 1995 onward. First and foremost, the importance of recent publications (from 2021) is highlighted, which shed light on the current state of information confrontation and trends in its scientific study. In the third stage, a preliminary screening of scientific publications was conducted by analyzing

the titles and the results obtained by researchers. The selected materials underwent a full textual analysis, which allowed us to determine their relevance. Works that did not meet the following criteria were excluded.

Thus, at the identification stage, 348 freely available publications in the scientific databases Google Scholar, Scopus, and Web of Science were processed and identified based on individual keywords.

After removing duplicates, 211 unique records were available for further processing.

During the screening of titles and research results, 135 papers that did not align with the research topic were rejected. 76 articles were selected for the next phase of text analysis.

In the next stage, as a result of a detailed analysis of the full texts of scientific sources, another 22 publications were blocked (they contained overly general results), were based on contradictory sources, and were not directly related to the topic of studying information wars.

Thus, 54 scientific sources directly relevant to the research goal and objectives of the article are proposed for the final synthesis (See Table 1).

Table 1. PRISMA method

Stage	Number of sources	Description of actions
Identification	348	Selection of publications by keywords in Google Scholar, Scopus, Web of Science databases
Duplicate removal	211	Removal of duplicate entries, unique sources left
Screening of titles and results	76	135 works that do not correspond to the topic were rejected; relevant articles were selected
Full text analysis	54	Another 22 publications were excluded due to lack of correspondence and connection with the topic
Final synthesis	54	The final pool of sources for the study was left

Source: Author's development

2.1 Data analysis

Based on the systematic method, the article identifies problems that have not been solved in scientific works and still need to be studied in detail. The comparative method was used to compare the data from the literature analysis and reflect on possible problems and ways to overcome the challenges of information wars. Based on the generalization, the results obtained are summarized, and the main manifestations of the Kremlin's aggressive policy in the information sphere, ways of responding to them and the necessary changes are characterized.

3. Results

3.1 The Role of Information Warfare in National Security (in the Example of Georgia)

The analysis of the factors leading to the Russian-Georgian conflict in 2008 suggests that the Soviet authorities deliberately fostered separatist movements in Georgia during the 20th century. Following the USSR's dissolution, political conflicts within Georgia escalated into open armed confrontations with its autonomies, Abkhazia and South Ossetia (the latter supported by Russia). Russian special services, upon Georgia's declaration of independence, orchestrated the creation of local separatist groups, managing them in both South Ossetia and Abkhazia (Vendil Pallin & Westerlund, 2009). During Eduard Shevardnadze's presidency in Georgia from 1992 to 2003, the government aimed for a strategic partnership with Russia, contingent on Russia recognizing Abkhazia as part of Georgia. This collaboration was intended to help Georgia resolve the Abkhaz conflict. Seeking to acquire arms that would later become Georgian property, Georgia signed an agreement to host Russian military bases on its territory (Gardner, 2013; Jozić *et al.,* 2016).

Russian mass media, politicians, and military officials increasingly propagated "information leaks" about Georgia's alleged aggression towards South Ossetia, indicating that Russia had already begun shaping public opinion for the impending conflict. This effort utilized various tools to prepare public opinion for the planned war. The August campaign saw targeted actions in cyberspace, including notable Distributed Denial of Service (DDoS) attacks. Reports indicate that the first DDoS attacks occurred on July 20, 2008, targeting the official website of the President of Georgia (Gamkrelidze, 2022). From August 7 to 16, 2008, powerful hacker attacks on the country's information resources, including the websites of the President of Georgia, the National Bank, and news agencies, resulted in their blockage.

One significant cyber operation involved hackers altering the exchange rate of the Georgian currency, the lari, leading to its devaluation. Western experts suggest that these cyberattacks also disrupted the exchange of information between units of the Georgian Armed Forces. Using sophisticated encryption methods and algorithms indicates a well-planned and coordinated operation, highlighting the cyber aspect as a distinct component of the Russian-Georgian information war. In response to these attacks, Georgian specialists blocked the work of South Ossetia's information resources on August 8, 2008. The next day, Georgia ceased broadcasting all Russian channels in the country and halted the operation of the .ru domain zone.

A successful cyber-attack destroyed the database of the Georgia online information resource and the website of the Rustavi-2 television company. The editors of Rustavi-2 accused the Russian Federation of waging an information war in response. Russian bloggers reported that the Russian Federation had blocked Georgian sites containing information about the situation in the country and its citizens. To inform the international community about the course of the conflict, Poland, Ukraine, and the USA provided their Internet resources (Zedelashvili, 2019). A well-executed information campaign, supported by other countries' leadership, allowed Georgia's power structures to portray the Russian Federation as an aggressor actively interfering in the internal affairs of a sovereign state. The conflict in August 2008 also saw 'intellectual duels' between bloggers from Russia and Western countries. This period is considered the first global information confrontation in the online environment, dubbed the 'global user-generated conflict'. The involvement of Runet users in openly propagandistic activities on the Internet yielded positive results. It marked the first instance of leveraging the potential of the blogosphere and social media networks in Russia for information warfare, with all actors and performers driven purely by patriotic motives and the national interests of the Russian Federation.

After the short-lived war in 2008, the Georgian authorities revised their national security strategy, focusing attention on cyber threats and countering hybrid challenges. Russian aggression demonstrated that in the 21st century, it is possible to destroy not only with weapons but also with other means. Figure 1 presents the leading innovative technologies used in the Russo-Georgian War.

Figure 1. Main Innovative Technologies Used in the 2008 War

Source: Author's development

Hence, as seen in Figure 1, cyberspace became an important component of national security during Georgia's conflict with Russia. This prompted the development of the National Cyber Security Strategy. In 2012, a new concept of national security was approved to cover the issues. The CERT Assistance Team has appeared to respond to computer incidents. The law created the Cybersecurity Bureau and the Bureau's Computer Incident Response Task Force to defend cyberspace.

3.2 The Role of Information Warfare in National Security (The Experience of Ukraine)

Modern experts highlight that Russia has been conducting systematic information propaganda since Ukraine gained independence. This propaganda was intensified during V. Yanukovych's presidency (Mudra & Sinkova, 2017). Additionally, it aimed to create a false media narrative of military events to garner support for Russia's actions among the populations of Southern and Eastern Ukraine. These tasks were executed through various communication channels, including traditional and electronic mass media, the Internet, and social networks.

The Russian Federation made significant efforts during the Russian-Georgian conflict and the Russian-Ukrainian war to shape the global narrative in its favour, leveraging its traditional strength in the information sphere. This was achieved through various means, including Western media and pro-Russian politicians worldwide (McCrory, 2020). Ukraine actively pursues an information policy aimed at combating Russian propaganda. This includes programs to inform the population about possible fake news from the enemy (Murinska et al., 2018). Since the end of February 2022, there has been extensive communication with the Ukrainian population, emphasizing that only official Ukrainian sources of information can be trusted. This has helped counter the traditional Russian tactic of spreading false information widely through social media and other public channels. From the early days of the Russian-Ukrainian war, journalists and Ukrainian military commanders have been providing prompt updates to the population about the successes and setbacks of the Ukrainian army. Moreover, the policy of openness in information sources has ensured objective news presentation in the global journalistic space (Romaniuk & Kovalenko, 2023). Ukraine's information policy has been notable for its journalists not concealing the brutality of the occupiers but, on the contrary, highlighting it separately. This has led to a clear understanding in Ukrainian society of the crimes of the Russian military and, consequently, a lack of acceptance of them and their slogans (Olivieri & Guadagno, 2024). From the perspective of the Russian leadership, the war was not supposed to last more than a few days. Therefore, as it might be assumed, there was no adequate information covering Russian aggression (Kominek et al., 2022). In the Russian-Ukrainian wars since 2014, innovative technologies for conducting information warfare have been constantly developing, as they were essential elements of its conduct. Social networks began to be actively used for propaganda purposes. In addition, artificial intelligence algorithms were used to analyze user behaviour and target specific groups. This was done in order to influence public opinion. With the help of such algorithms, the automatic creation of personalized messages and the appropriate selection of materials or content were carried out. The use of bot farms and trolls has mainly spread. Bots play the role of special automated account requests in social networks that can spread false information. At that time, trolls acted as special organizational groups that wrote provocative comments. Deepfake technology also plays a vital role in the current war. In particular, they make it possible to use artificial intelligence to create fake videos or audio recordings (Vanorio, 2023; Upadhyay, 2023).

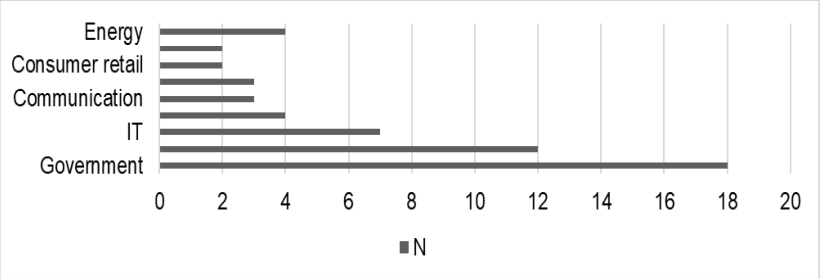

Figure 2. The Number of Cyber Attacks in Different Areas of Ukraine Since the Beginning of the Full-scale Invasion

Source: Cyber-attacks during the Russian invasion of Ukraine (2022)

However, in 2022, cyber attacks began to be used more actively. They are related to the hacking of government websites, the theft of data or the hacking of critical infrastructure. Since the beginning of the full-scale

intrusion (in the first months), there have been almost 20 attacks on government portals. Media, IT offices and other institutions were also affected (see Figure 2).

Phishing and spoofing were also used in Ukraine to spread fake news through e-mails or social networks that looked like official sources. Extensive data analysis is another critical technology in the hybrid war with Ukraine. In particular, big data makes it possible to analyze vast arrays of user data and identify patterns of behaviour and interests. This technology has been used to target specific populations that may be less resistant to manipulation (Thornton, 2015). Psychological operations (PsyOps) also became an important technology that was actively used by the Russians from the beginning of the full-scale war (Walsh *et al.,* 2023). PsyOps performs the role of special psychological operations aimed at psychological influence on the enemy through the manipulation of information. In Ukraine, they were used to spread fear, panic or despair through the media (Kozak *et al.,* 2024a; Kozak *et al.,* 2024b).

Additionally, Ukrainian media's internal information activities have increased Ukrainian' awareness, as they have learned to resist propaganda and distinguish false information. Moreover, during the Russian-Ukrainian war, this trust did not decrease but on the contrary, it increased despite all the information challenges.

Ukraine has taken several legislative steps to counter Russia's aggression. Here are some of them (Kobko, 2023; Dekhtiar, 2019).

Ukraine has implemented various laws that impose sanctions on Russian entities and individuals who support aggression and the information war against Ukraine. The Media Law, adopted in 2021, regulates media activities and establishes standards to prevent the dissemination of Russian propaganda. The Law on Cinema and Television also restricts Ukrainian TV channels from broadcasting Russian films and programs. The legal framework also includes a ban on Russian social networks within Ukraine. These measures are designed to bolster national security and limit Russia's influence on Ukraine's domestic matters.

3.3 The tactics of Russia's Information Warfare in the wars with Georgia and Ukraine

In both the 2008 attack on Georgia and the ongoing invasion of Ukraine, Russia vehemently denied its role as the aggressor. Moscow strategically crafted vague or justifying names for their military actions to bolster this denial (Watzlawick, 2016; Narvaez Barrera, 2025). In 2008, it was dubbed 'Operation to Force Peace', while in 2022, it was branded as a "Special Military Operation". Despite these euphemisms, the underlying aggression was purportedly justified by Russia's alleged concern for oppressed groups, such as Ossetians or residents of Donbas, to whom Russian passports had been distributed beforehand.

Table 2. Russian Mechanisms of Conducting Information Warfare Against Georgia and Ukraine

Aspect	2008 Attack on Georgia	2014\2022 Invasion of Ukraine
Denial of Aggression	Russia vehemently denied being the aggressor.	Russia vehemently denied being the aggressor.
Justifying Names	'Operation to Force Peace'	'Special Military Operation'
Pretext for Aggression	Concern for oppressed groups (Ossetians)	Concern for oppressed groups (Donbas residents)
Proxy Groups	Moscow relied on cultivated groups for support.	Moscow relies on cultivated groups for support.
Passportization	Russian passports distributed to Ossetians.	Russian passports distributed to Donbas residents.
Propaganda Russia fighting against the criminal regime.	Georgia portrayed as fascist state. At the official level, it was stated that Russia was not at war with the Georgian people, but with its "criminal government."	Ukraine portrayed similarly. Similar wording about Russian military fighting with a "fascist," criminal government has been echoing about Ukraine since 2014.

Atrocity Narratives	Accusations of Georgian atrocities propagated.	Accusations of Ukrainian atrocities spread.
Accusations of Genocide	Russia accused Georgia of genocide in South Ossetia.	Russia accused Ukraine of genocide in Donbas.
Blaming the West	Accused US of supplying weapons to Georgia.	Accused US of involvement in Ukraine.
Discrediting Leaders	Saakashvili attacked personally.	Zelensky portrayed as weak and inadequate.
Stoking Interethnic Tensions	During the conflict with Georgia, Russian criminal chronicles deliberately emphasized the Georgian ethnic origin of the criminals.	Similarly, since 2022, Ukrainians have been accused of drug trafficking in the territory of the Russian Federation. Hypocritical statements about friendly feelings towards the Ukrainian people are made in parallel with the destruction of Ukrainian-language books and a persistent narrative that Ukrainians as a separate nation should be destroyed, and their children should be re-educated as Russians.

Source: Author's development

Table 1 outlines Russian mechanisms of conducting information warfare against Georgia and Ukraine during the 2008 attack on Georgia and the 2014/2022 invasion of Ukraine. In both cases, Russia denied being the aggressor and justified its actions with concerns for oppressed groups. Moscow used proxy groups to support and distribute passports to specific populations. In addition, Russia used various innovative information warfare technologies in both cases. These technologies aimed to manipulate the population's consciousness and had a psychological impact. However, compared to the 2008 war, these technologies have greatly expanded (see Table 3).

Table 3. Comparative Table of Innovative Information Warfare Technologies

Technologies	**Georgia**	**Ukraine**
Social networks	3	3
Algorithms of artificial intelligence	0	1
bot farms	2	3
Deepfake	0	1
Cyber attacks and hacking tools	3	3
Phishing / spoofing	2	2
Big Data Analysis	1	2
Network anomalies	0	1
Information traps	2	2
PsyOps	0	2
Fakenews	3	3
Trolls	3	3

Source: Author's development

Table Commentary: 0 = technology is absent / not applied 1 = limited or experimental application 2 = moderate application 3 = widespread / systematic application.

As seen from this table, the innovative technologies of warfare have expanded significantly. Current innovations significantly affect the transformation of information warfare methods and influence public opinion.

Overall, based on Table 2 and Table 3, some parallels and key differences can be established regarding the development of a generalizing typology of information warfare strategies. First and foremost, in both cases of Ukraine and Georgia, a powerful arsenal of the main tools of Russian propaganda has been demonstrated (extreme denial of aggression, the importance of fabricated narratives about "genocide" or "protection of civilians," the use of military proxy groups, passportization policy, etc.). At the same time, the current state of the technological environment and new possibilities of information practices have indicated the emergence of new methods related to digitalization and algorithmic influence.

Based on these results, we can identify several levels of information warfare:

1 Basic practices in performing manipulations.

2 Modern digital tools for spreading information influence.

3 Application of innovative algorithmic tools.

Using a similar three-level model allows for a general comparison of aggression against Georgia and Ukraine and the extrapolation of the findings to other regions, as the application of such a system is possible in the future. However, there are potential ways to protect against this: at the level of new actions in political communication (debunking mythical narratives, countering the exposure of false messages), at the digital level (countering cyberattacks, countering and blocking botnets, avoiding information traps), and at the level of algorithmic protection (automatic identification of deepfakes, control over disinformation). Thus, this typology of strategies and levels of information warfare made it possible to identify the main Russian approaches from 2008 to 2022, forming the basis for further comparative studies.

4. Discussions

Therefore, this study aimed to identify the main trends in using innovative technologies for information warfare. The study results demonstrated that a feature of conducting information wars is using various tools and innovative technologies. In addition, Russia used similar scenarios to conduct a hybrid war. In particular, this concerns propaganda, the passporting of the population, and the introduction of proxy groups. Accordingly, this study correlates with the results of other scientists. As research showed by August 2008, Georgia had lost control over most of the territories of Abkhazia and the predominantly Ossetian-populated Tskhinvali region, which had seceded during the separatist conflicts of the early 1990s, aided by Russian 'hybrid' forces (Chandra & Pprasad, 2023; Deibert *et al.,* 2012; Dunlop, 2022). This situation bore similarities to the war in Donbas and the establishment of the so-called 'DPR' and 'LPR' in 2014. These conclusions also correlate with the data obtained (Häggström, 2021; Haltsova *et al.,* 2024; Kozlovskyi *et al.,* 2022; 2024; Mansoor, 2022). In both instances, Russia masqueraded as a mediator and peacekeeper yet ultimately resorted to open aggression and instigated interstate warfare (Iasiello, 2017; Tsekhmister, 2024; Yuryk *et al.*, 2023).

Under the guise of 'protecting peaceful citizens', who conveniently happened to be Russian citizens, Moscow relied on proxy groups it had cultivated, portraying them to the world as champions of cultural identity and freedom from oppression.

The results also indicate a particular aspect of modern hybrid warfare - the passporting of the population. According to modern works, the passportization of Ossetians by Russia, coupled with claims of their "protection", served as a pretext for attacks on Georgia that extended far beyond the Tskhinvali region. Russian forces bombed the oil port in Poti, destroyed the railway infrastructure, and ventured deep into Georgian territory. Simultaneously, Russia asserted its 'liberation' of Upper Abkhazia, although there had been no aggression from Georgia (Fedorchak, 2024; Kuzheliev *et al.,* 2023; Muradov, 2022; Ventre, 2016).

The next task is related to the characteristics of the leading technologies. Therefore, the study demonstrated that Russia used various innovative technologies to wage war: artificial intelligence, bot farms, trolling, psychological operations, Phishing/spoofing, and fake news. These results also correlate with other works in which the features of conducting modern hybrid wars are characterized. However, the most critical challenge has become the conduct of cyber attacks. This correlates with current research emphasizing the importance of creating a cyber-safe space (Douglas, 2024; Iasiello, 2017; Ventre, 2016).

The proposed results actively confirm a certain stereotypical nature of Russian information strategies. At the same time, some researchers have emphasized that the effectiveness of disinformation campaigns is lower in countries with a stable democratic society, which also implies higher levels of media literacy and media pluralism (Kobko, 2023). The Ukrainian side was able to partially confirm this thesis. Despite the large-scale information campaign by Russian media after 2014, their effect proved to be more limited. The Georgian case showed different results, as the weakness of democratic institutions contributed to deeper destabilization. At the same time, other scholars have highlighted the increasing functions of digital diplomacy, which should be a response to information

challenges (Muñoz Plaza *et al.,* 2024). The proposed results demonstrated that Ukraine's active application of digital diplomacy after 2014 has become an effective response to certain tools of Russian fake news.

The last task concerned defining differences in the information warfare systems in Georgia and Ukraine. Accordingly, it was established that, in comparison with 2008, the arsenal of innovative technologies has increased and improved significantly. This correlates with a number of modern studies, which emphasize the development of modern innovative means of warfare (Huang, 2024; Kestner, 2024; Muñoz Plaza *et al.,* 2024).

The limitations of this study concern the selection of only modern literature. Therefore, the work is not a study of the peculiarities of the historical development of information wars. In addition, primarily literature in English (sometimes Ukrainian) is included. This study did not include sources in other languages. Accordingly, these limitations have opened up new perspectives for research. In the future, the main emphasis should be on the historical development of hybrid wars. Analysis of quantitative indicators of conducting cyberattacks and manipulations in social networks is also a promising direction. However, given the war in Ukraine, this information is not yet widely available. Despite these limitations, the scientific value of this study is excellent, as this work demonstrated a comparison of the features of the use of innovative technologies in the war on the territory of Georgia and Ukraine.

5. Conclusions

The role of information warfare in national security is a critical aspect of modern conflict. Both countries have faced challenges from Russian information warfare, which has been used as a tool to destabilize their governments, sow internal divisions, and justify military aggression. This approach has evolved in the digital age, with the proliferation of social media and online platforms enabling more sophisticated and widespread dissemination of false narratives. In addition, the study determined that the leading technologies used to conduct information warfare were extensive data analysis, artificial intelligence, fake news, bot farms, trolling, Phishing/spoofing, and PsyOps. However, hacker attacks and cyber-attacks directed at various structures, government websites, media, IT offices, energy, and communication become especially common.

In addition to the purely national dimension, specific strategic implications can be proposed. First and foremost, there is a need to significantly strengthen the EU and NATO's cybersecurity: additional coordination in countering large-scale information campaigns and hybrid challenges will help secure this area. Secondly, the Ukrainian and Georgian experiences have highlighted the importance of developing new international legal norms to counter the spread of disinformation and establish accountability for such acts. Both cases are examples for other small democracies, as in the current circumstances of globalization, an information campaign can be planned and implemented against any country. Effective steps include combining legislative initiatives, implementing measures to improve media literacy, and using digital diplomacy as an effective tool.

In conclusion, Ukraine and Georgia's experiences highlight the importance of information warfare in contemporary national security challenges. As technology advances, so must the strategies for countering disinformation and propaganda. By understanding and addressing the tactics used by hostile actors, countries can better protect their democratic institutions and safeguard their sovereignty.

References

Amilakhvari, L., & Baghaturia, O. (2024). Russia's militaristic rhetoric, imperialism, and expansion. In *Dealing with regional conflicts of global importance*. IGI Global, 161–181. https://doi.org/10.4018/978-1-6684-9467-7.ch008

Bartnicki, A.R., Kużelewska, E., Ożóg, M. (2023). Information and information technologies in the 2022 Russian-Ukrainian war. In *War in Ukraine: Media and emotions*, *Springer Nature* Switzerland. https://doi.org/10.1007/978-3-031-37608-5_3

Blănaru, M. (2024). The need for an integrated model of smart warfare. *Bulletin of "Carol I" National Defence University, 13*(1), 44–62. https://doi.org/10.1007/978-3-031-37608-5_3

Chandra, R., Prasad, P.W.C. (2023). Cyber warfare: Challenges posed in a digitally connected world: A review. In *Lecture notes in electrical engineering*, *Springer Nature*, Switzerland. https://doi.org/10.1007/978-3-031-29078-7_16

Chong, A. (2014). Information Warfare?: The Case for an Asian Perspective on Information Operations. *Armed Forces & Society,* 40(4), 599–624. https://doi.org/10.1177/0095327X13483444

Church, W. (2000). Information warfare. *International Review of the Red Cross, 82*(837), 205–216. https://doi.org/10.1017/S1560775500075489

Cybulsky, A.V. (2022). War in Ukraine. *Kidney International,* 102(3), 669. https://doi.org/10.1016/j.kint.2022.06.014

Deibert, R.J., Rohozinski, R., Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue, 43*(1), 3–24. https://doi.org/10.1177/0967010611431079

Dekhtiar, V. (2019). Ukrainian studies: From ideology to identity politics. *Ukrainian Studies,* (2), 31–39. https://doi.org/10.30840/2413-7065.2(71).2019.172382

Douglas, M., Reith, M. (2024). A survey of learning technology integration in information warfare education. *European Conference on Cyber Warfare and Security, 23*(1), 148–156. https://doi.org/10.34190/eccws.23.1.2403

Dunlop, J.B. (2022). The August 2008 Russo-Georgian war. In *Russia and its near neighbours*. Palgrave Macmillan. https://doi.org/10.1057/9780230390164.0011

Fedorchak, V. (2024). Information and cyber aspects of the war. *In The Russia-Ukraine*, Routledge. https://doi.org/10.4324/9781003351641-9

Gamkrelidze, T. (2022). Georgia's external frontier on Russia sedimented and unmalleable: Engagement politics and the impact of the three-tier warfare. *Journal of Contemporary European Studies*, 31(2), 536-555. https://doi.org/10.1080/14782804.2021.2023485

Gardner, H. (2013). Ramifications of the August 2008 Georgia-Russia war. In *NATO expansion and US strategy in Asia*. Palgrave Macmillan US. https://doi.org/10.1057/9781137367372_5

Häggström, H. (2021). Hybrid threats and new challenges for multilateral intelligence cooperation. In *Hybrid warfare*, Tauris. https://doi.org/10.5040/9781788317795.0015

Haltsova, V.V., Volodina, O.O., Hordieiev, V.I., Samoshchenko, I.V., Orobets, K.M. (2024). Analysis of criminal law on ecocide: A case study of war in Ukraine. *Revista Kawsaypacha: Sociedad y Medio Ambiente*, (14), D—013. https://doi.org/10.18800/kawsaypacha.202402.D013

Horobets, I.V., Martyinov, A.Y., Braychevskaya, E.A., Krupenya, I.M., Sliusarenko, I.Y. (2022). Political culture and identity politics in the Ukrainian society. *Journal of Community Positive Practices, 22*(4), 65–81. https://doi.org/10.35782/JCPP.2022.SI.1.6

Huang, J. (2024). Information warfare in the digital age: Legal responses to the spread of false information under public international law. *Journal of Education, Humanities and Social Sciences, 28*, 176–184. https://doi.org/10.54097/46jmtq31

Hutchinson, W. (2002). Concepts in information warfare. *Logistics Information Management, 15*(5/6), 410–413. https://doi.org/10.1108/09576050210447109

Iasiello, E.J. (2017). Russia's improved information operations: From Georgia to Crimea. *The US Army War College Quarterly: Parameters, 47*(2), 51–63. https://doi.org/10.55540/0031-1723.2931

Jozić, J., Barić, S., & Barić, R. (2016). Hybrid warfare—Cases of Croatia and Ukraine. *Vojenské Rozhledy, 25*(5), 104–122. https://doi.org/10.3849/2336-2995.25.2016.05.104-122

Kernen, B., & Sussex, M. (2012). The Russo-Georgian war. In M. Sussex (Ed.), *Conflict in the former USSR*, Cambridge University Press. https://doi.org/10.1017/CBO9780511980565.006

Kestner, P. (2024). Survival in cyberspace: Strategies for every individual. In *The art of cyber warfare*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-43879-1_8

Kobko, Y.V. (2023). Information warfare and disinformation: Impact on the national security of Ukraine. *Legal Novels, (20)*, 141–147. https://doi.org/10.32782/ln.2023.20.20

Kominek, Ł., Staśkiewicz, U., Maciąg, M. (2022). Russia-Ukraine: War? New war? Old war? *National Security Studies, 26*(4), 11–20. https://doi.org/10.37055/sbn/152883

Kozak, N., Rudynskyi, O., Kozak, D. (2024a). Regulatory and legal aspects of military doctors and pharmacists training in wartime: Continuous professional development at the faculty of retraining and advanced training of the Ukrainian Military Medical Academy. *Ukrainian Journal of Military Medicine*, *5*(3), 30–38. https://doi.org/10.46847/ujmm.2024.3(5)-030

Kozak, N.D., Rudynskyi, O.V., Verba, A.V., Asaulenko, A.A., Kozak, D.O. (2024b). Potential and real dangers of the chemical warfare agents use during the full-scale invasion into Ukraine. *Wiadomości Lekarskie*, *77*(11), 2186–2192. https://doi.org/10.36740/wlek/197094

Kozlovskyi, S., Petrunenko, I., Mazur, H., Butenko, V., Ivanyuta, N. (2022). Assessing the probability of bankruptcy when investing in cryptocurrency. *Investment Management and Financial Innovations,* 19(3), 312–321. https://doi.org/10.21511/imfi.19(3).2022.26

Kuzheliev, M., Zherlitsyn, D., Nechyporenko, A., Lutkovska, S., Mazur, H. (2023). Distance learning as a tool for enhancing university academic management processes during the war. *Problems and Perspectives in Management,* 21(2), 23–30. https://doi.org/10.21511/ppm.21(2-si).2023.04

Mansoor, P.R. (2022). Introduction. Hybrid Warfare in History. *Cambridge University Press*. https://doi.org/10.1017/CBO9781139199254.001

McCrory, D. (2020). Russian electronic warfare, cyber and information operations in Ukraine. *The RUSI Journal,* 165(7), 34–44. https://doi.org/10.1080/03071847.2021.1888654

Mereniuk, K., & Parshyn, I. (2024). Military units and symbolism: Utilization of imagery from medieval Rus in the Russian-Ukrainian war. *Trames: Journal of the Humanities and Social Sciences, 28*(3), 293–312. https://doi.org/10.3176/tr.2024.3.05

Mudra, I., & Sinkova, Y. (2017). Tools of information against war in Ukraine. *Bulletin of Lviv Polytechnic National University: Journalistic Sciences, 2017*(1), 42–47. https://doi.org/10.23939/sjs2017.01.042

Muñoz Plaza, F., Hernández San Román, I., Sotelo Monge, M.A. (2024). A technical exploration of strategies for augmented monitoring and decision support in information warfare. In *ARES 2024: The 19th International Conference on Availability, Reliability and Security*. ACM. https://doi.org/10.1145/3664476.3670922

Muradov, I. (2022). The Russian hybrid warfare: The cases of Ukraine and Georgia. *Defence Studies*. https://doi.org/10.1080/14702436.2022.2030714

Murinska, S., Aleksandrova, O., & Dodonov, R. (2018). Information warfare: Future challenges of Latvia and Ukraine. *Skhid, (5)*, 66–72. https://doi.org/10.21847/1728-9343.2018.5(157).148661

Narvaez Barrera, M.J. (2025). Transformation of administrative management through emerging technologies and digital innovation. *Diginomics*, 4, 204. https://doi.org/10.56294/digi2025204

Office for Budget Responsibility. (2022). *Cyber-attacks during the Russian invasion of Ukraine*. https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/

Olivieri, A., & Guadagno, R. (2024). Strategies for combating adversarial information operations: Theory and practical applications. *European Conference on Cyber Warfare and Security, 23*(1), 341–347. https://doi.org/10.34190/eccws.23.1.2435

Panda, B., & Giordano, J. (1999). Defensive information warfare. *Communications of the ACM, 42*(7), 30–32. https://doi.org/10.1145/306549.306559

Parshyn, I., & Mereniuk, K. (2024). A modern view of the European vector of the military development of Ukrainian lands in the 13th–14th centuries: Prospects for future historiographical studies. *Futurity of Social Sciences*, 61–78. https://doi.org/10.57125/FS.2023.09.20.05

Romaniuk, O., Kovalenko, I. (2023). Information means of warfare. *Visnyk of Kharkiv State Academy of Culture, (63)*, 7–18. https://doi.org/10.31516/2410-5333.063.01

Sashchyk, H., Rykhlik, V. (2022). Information component of Russia's hybrid war against Ukraine. *Politology Bulletin*, (89), 133–146. https://doi.org/10.17721/2415-881x.2022.89.133-146

Thornton, R. (2015). The changing nature of modern warfare. *The RUSI Journal, 160*(4), 40–48. https://doi.org/10.1080/03071847.2015.1079047

Tsekhmister, Y. (2024). War, education and development: a pedagogical response to the challenges of modernity. *Academia*, (35–36), 1–8. https://doi.org/10.26220/aca.4999

Upadhyay, P. (2023). Information warfare and digitalization of politics in a globalized world. *Journal of Political Science, 23*(1), 1–30. https://doi.org/10.3126/jps.v23i1.52280

Van Niekerk, B. (2024). Cyber operations in peace and war: A framework for persistent engagement. *International Conference on Cyber Warfare and Security, 19*(1). https://doi.org/10.34190/iccws.19.1.2092

Vanorio, F. (2023). Technological innovations: A new model of geopolitical digital relations from welfare to warfare?. *Monetary Policy Normalization. Contributions to Economics,* Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-38708-1_9

Vendil Pallin, C., Westerlund, F. (2009). Russia's war in Georgia: Lessons and consequences. *Small Wars & Insurgencies, 20*(2), 400–424. https://doi.org/10.1080/09592310902975539

Ventre, D. (2016). Concepts and theories: Discussions. *In Information warfare, John Wiley & Sons*. https://doi.org/10.1002/9781119004721.ch4

Walsh, M., Seher, I., Prasad, P.W.C., Elchouemi, A. (2023). The integration and complications of emerging technologies in modern warfare. Innovative Technologies in Intelligent Systems and Industrial Applications, Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-29078-7_40

Watzlawick, A. (2016). An analysis of the choice and use of weapons by Russia and Georgia in the 2008 South Ossetia conflict. *University of Cape Town.*

Yuryk, O., Holomb, L., Konovalova, L., Vivsyannuk, V., Tsekhmister, Y. (2023). Assessment of the impact of artificial intelligence technologies on the development of Ukrainian medicine in war conditions. *International Journal of Chemical and Biochemical Sciences*, *24*(5), 206–211.

Zedelashvili, T. (2019). Geopolitical contours of modern information warfare: Russian-US confrontation line from Baltic Sea to Black Sea. *Ante Portas—Studia nad Bezpieczeństwem, 2*(13), 119–131. https://doi.org/10.33674/20199

Does this article screen for similarity?

Yes

Conflict of Interest

The author have no conflicts of interest to declare. There is also no financial interest to report. The author certifies that the submission is original work and is not under review at any other publication.

About the License

Cite this Article

Leyla Derviş, Innovative Technologies in Information Warfare as a Means of Protecting National Interests of Ukraine and Georgia: A Literature Review, Asian Journal of Interdisciplinary Research, 8(4), (2025) 1-12. https://doi.org/10.54392/ajir2541