The Impact of Artificial Intelligence on hybrid warfare: Case of Russia-Ukraine war

By

Muhammad Derfish Ilyas

The University of the Cumberlands, Kentucky, USA

Abstract

The stimulus to carry out this research is to identify how Artificial Intelligence (AI) can impact hybrid warfare. Hybrid Warfare (HW) has become a popular yet controversial term in academic and military discourse. Its popularity lies mainly in capturing the form of struggle, which features a combination of new technologies and fanatic fighting styles by non-state actors, and later the 'covert' operations of state actors that use deniable or paramilitary forces and incremental tactics to achieve the political aim.

The research utilizes a hybrid warfare model proposed by Erik Reichborn-Kjennerud and Patrick Cullen, which is based on five instruments, which are military, political, economic, civil, and informational (MPECI) (Yan, 2020). It analyzes how artificial Intelligence is impacting these instruments in the Russia-Ukraine war.

The study reviewed the published literature in this context and extracted its findings in the context of the Russia-Ukraine war. Results will benefit the state and non-state actors of countries around the globe. Non-state actors includes NGO, financial institutions and other independent institutaitons. Findings will also help the international criminal justice system so they can identify how hybrid warfare techniques are used by the state and non-state actors.

Keywords: *Russia, Ukraine, War, Hybrid Warfare, Artificial Intelligence, AI*

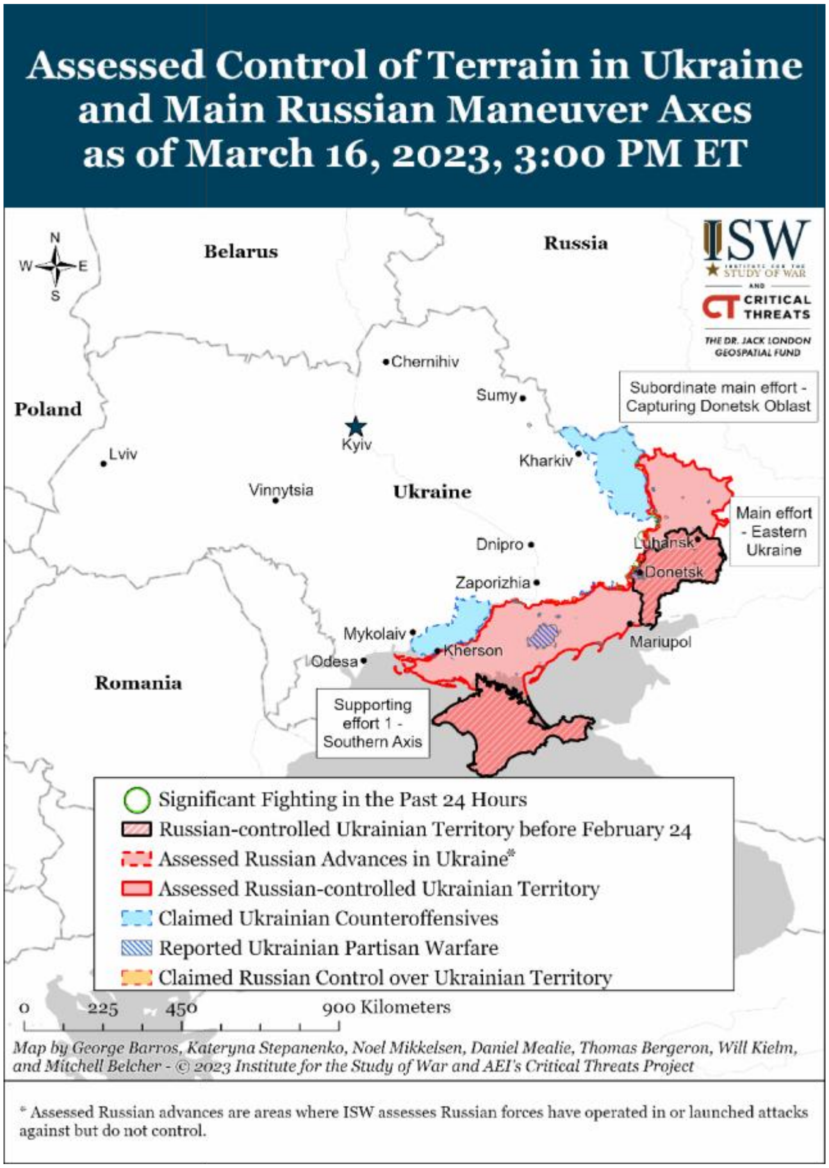
Introduction

Hybrid warfare (HW) has become a popular and widely discussed term in recent years, particularly in the context of conflicts involving state and non-state actors (Libiseller, 2023). Hybrid warfare is a complex form of warfare involving multiple instruments, such as military, political, economic, civil, and informational (MPECI), to achieve a political aim (Yan, 2020). This type of warfare combines a range of military and non-military tactics, including cyberattacks, propaganda, and subversion, to achieve strategic objectives (Mumford, 2023). With the increasing integration of technology in modern warfare, the impact of Artificial Intelligence (AI) on hybrid warfare has become a topic of great interest and concern for policymakers, military strategists, and academics alike (Mattingsdal, 2023). This research paper aims to explore the impact of AI on hybrid warfare, using the case of the ongoing Russia-Ukraine war as a case study.

Background

Hybrid warfare tactics have also been used in other conflicts around the world, including in Syria, Yemen, and Afghanistan (Khorram-Manesh, 2022). According to Gasztold (2022), these tactics have raised concerns about the effectiveness of traditional military strategies and the potential for non-state actors to disrupt global security and stability.

The Russia-Ukraine war is an ongoing conflict that began in 2014 after the annexation of Crimea by Russia (Mbah, 2022). The war has since escalated, with both sides using various tactics to achieve their political objectives (Ociepa-Kicińska, 2022). As per Kurapov et al. (2022), the use of hybrid warfare tactics in the Russia-Ukraine conflict has been well documented. The battle has witnessed the use of paramilitary forces, deniable operations, cyberattacks, propaganda, and disinformation campaigns (Vorburgg, 2022). These tactics have enabled both sides to achieve their objectives while also making it difficult for the international community to respond effectively (Armitage, 2022).


Assessed Control of Terrain in Ukraine and Main Russian Maneuver Axes as of March 16, 2023, 3:00 PM ET
ISW INSTITUTE FOR THE STUDY OF WAR AND CT CRITICAL THREATS
THE DR. JACK LONDON GEOSPATIAL FUND
N
W
E
S
Belarus
Russia
Poland
Ukraine
Romania
Chernihiv
Sumy
Kyiv
Lviv
Kharkiv
Vinnytsia
Dnipro
Luhansk
Donetsk
Zaporizhia
Mykolaiv
Kherson
Odesa
Mariupol
Subordinate main effort - Capturing Donetsk Oblast
Main effort - Eastern Ukraine
Supporting effort 1 - Southern Axis
○ Significant Fighting in the Past 24 Hours
▨ Russian-controlled Ukrainian Territory before February 24
▨ Assessed Russian Advances in Ukraine*
🟥 Assessed Russian-controlled Ukrainian Territory
▨ Claimed Ukrainian Counteroffensives
▨ Reported Ukrainian Partisan Warfare
▨ Claimed Russian Control over Ukrainian Territory
0 225 450 900 Kilometers
Map by George Barros, Kateryna Stepanenko, Noel Mikkelsen, Daniel Mealie, Thomas Bergeron, Will Kielm, and Mitchell Belcher - © 2023 Institute for the Study of War and AEI's Critical Threats Project
* Assessed Russian advances are areas where ISW assesses Russian forces have operated in or launched attacks against but do not control.

Source –(Hird, 2023)

According to Hird (2023), the red-colored areas on maps are those controlling Russia. Similarly, the dotted red colors on the map are those in which Russia is advancing to get control. The green circles on the map are areas where significant fighting has been going on forthe past 24 hours.

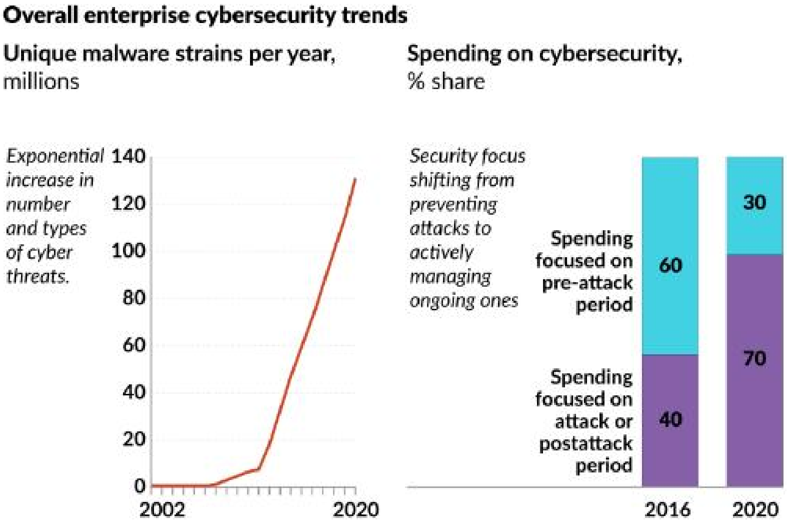
According to Patel (2022),hybrid warfare tactics have been used extensively by both Russia and Ukraine in this conflict. Russia has been accused of using covert military operations, propaganda, and cyberattacks to support separatist forces in eastern Ukraine (Burkle, 2022). Conversely, Ukraine has used unconventional tactics such as volunteer battalions and social media campaigns to mobilize support for its cause.

The use of hybrid warfare tactics in the Russia-Ukraine conflict has resulted in significant human and economic costs. According to the United Nations, the conflict has resulted in over 13,000 deaths and the displacement of 1.6 million people (Solmaz, 2022). The conflict has also caused significant damage to both countries' infrastructure and economy, with estimates suggesting that the total cost of the conflict could reach up to $100 billion (Muradov, 2022). Since the full–scale invasion of Ukraine on February 24, 2022, the Ukrainian Ministry of Health has reported that the Russians have damaged 788 medical facilities and "turned another 123 into piles of stones" (Kricorian, 2022).

Russia has been engaging in hybrid warfare tactics against Ukraine, which involve a combination of traditional military tactics with unconventional methods such as cyberattacks, propaganda, and paramilitary forces. These tactics have been used to achieve political objectives, including the annexation of Crimea and the destabilization of eastern Ukraine.

Russia has been using hybrid warfare tactics in Ukraine since 2014, including the use of propaganda, cyber-attacks, covert operations, and the deployment of paramilitary forces (Khorram-Manesh, 2022). One of the main goals of Russia's hybrid warfare tactics is to destabilize Ukraine politically and economically, making it more susceptible to Russian influence.

Russia's hybrid warfare tactics involve a combination of conventional military operations, paramilitaries, information warfare, and "little green men" (Russian special forces disguised as local separatists). These tactics have been used to target Ukrainian civilians, infrastructure, and the economy. Human rights violations, such as torture and extrajudicial killings, have been documented by the UN and other international organizations. In addition, Russia has violated international law by annexing the Crimea region. Itcurrently violates the Minsk II agreement, signed in 2015, which calls for a ceasefire and the withdrawal of heavy weapons (Wells, 2022). Russia has also used economic measures such as trade embargoes, energy cuts, and currency manipulation to weaken the Ukrainian economy (Morejón-Llamas, 2022). Finally, Russia has used proxies, including pro-Russian separatists in eastern Ukraine, to carry out military operations and destabilize the Ukrainian government.



Source – (Umbach, 2022)

According to the above figure, Russia is also facing cyberattacks, which supersedes t Moscow's superiority in cyberattacks. These statistics from Umbach (2022) indicate an exponential increase in cyberattacks on Russia. These figures also suggest that as of 2020, Russia is spending more on focused attacks or post-attack periods.

Russia's use of hybrid warfare tactics in Ukraine has led to numerous violations of international law and human rights. For example, the deployment of paramilitary forces in Ukraine violates Ukraine's territorial integrity and sovereignty, as well as international law (Morejón-Llamas, 2022). Additionally, Russia's use of cyber-attacks and propaganda to influence the outcome of the conflict violates international norms of non-interference in the internal affairs of other countries.

One of the violations committed by Russia in this context is the destruction of healthcare facilities in Ukraine. This is a grave violation of the Geneva Convention and constitutes a war crime. Despite existing international humanitarian and human rights laws, Russia has shown a disregard for these laws. It has withdrawn from Article 90 of Protocol I of the Geneva Convention, undermining its commitment to upholding these laws. Such actions may have long-term implications for international justice and the accountability of war criminals.

This research paper will use a hybrid warfare model proposed by Erik Reichborn-Kjennerud and Patrick Cullen, which focuses on the five instruments of hybrid warfare, to analyze the impact of AI on hybrid warfare in the context of the Russia-Ukraine conflict. The study will utilize the substantive literature review (SLR) technique to review published material and extract findings relevant to the context of the ongoing conflict.

Problem

Hybrid warfare has become a significant challenge for states worldwide because it can cause damage without conventional military action. As new technologies continue to emerge, the potential impact of Artificial Intelligence on hybrid warfare is a growing concern (Solmaz, 2022). However, Morejón-Llamas (2022) and Wells (2022) lack research on the specific ways AI is being utilized in hybrid warfare and its impact on the instruments of MPECI.

The practical problem identified in this research is the need to understand how AI is being used in hybrid warfare and its potential implications for national security (Kricorian, 2022). Additionally, there is a lack of knowledge on how AI can be leveraged to counteract hybrid warfare tactics (Muradov, 2022).

Several research studies Burkle (2022), Patel (2022) is conducted on the hybrid warfare and use of AI in the case of Russia and Ukraine war, however limited studiesMorejón-Llamas (2022) have found which have used MPECI hybrid warfare model proposed by Erik Reichborn-Kjennerud and Patrick Cullen (Reichborn-Kjennerud & Cullen, 2016).The research gap in this area is the lack of studies that have explored the specific ways in which AI is being utilized in hybrid warfare, particularly in the context of the Russia-Ukraine war (Wells, 2022). The problem statement for this research paper is, "The lack of understanding of how Artificial Intelligence is being utilized in hybrid warfare and its impact on the instruments of MPECI in the context of the Russia-Ukraine war necessitates a substantive literature review to inform future research and national security strategies."

Research Question

How Artificial Intelligence is impacting the hybrid warfare and its five instruments which are military, political, economic, civil, and informational (MPECI) in Russia – Ukraine war.

Research Objectives

- To identify how Artificial Intelligence impacts the military instrument of hybrid warfare in the Russia – Ukraine war.
- To identify how Artificial Intelligence impacts the political instrument of hybrid warfare in the Russia – Ukraine war.
- To identify how Artificial Intelligence impacts the economic instrument of hybrid warfare in the Russia – Ukraine war.
- To identify how Artificial Intelligence impacts the civil instrument of hybrid warfare in the Russia – Ukraine war.
- To identify how Artificial Intelligence impacts the informational instrument of hybrid warfare in the Russia – Ukraine war.

Significance

The significance of this research study lies in its potential to shed light on the impact of Artificial Intelligence on hybrid warfare, using the case of the Russia-Ukraine war as an example. Hybrid warfare is a complex and evolving form of warfare that has become increasingly prevalent in modern times, and understanding how AI is impacting the various instruments of hybrid warfare can provide valuable insights for both state and non-state actors.

The study's use of the MPECI model proposed by Reichborn-Kjennerud and Cullen provides a framework for analyzing the impact of AI on hybrid warfare, and the use of the substantive literature review technique allows for a comprehensive analysis of existing research in this area. The findings of this study can inform policy and decision-making at both national and international levels, particularly in the context of the ongoing Ukraine conflict and the potential for future hybrid warfare conflicts.

Furthermore, the study's potential to inform the international criminal justice system about the use of hybrid warfare tactics by state and non-state actors is significant. With the ICC announcing its jurisdiction over potential war crimes in Ukraine, understanding the ways in which hybrid warfare is being used can aid in the identification and prosecution of perpetrators of such crimes. Overall, this research study can contribute to a better understanding of the impact of AI on hybrid warfare and its implications for international security and justice.

Literature review

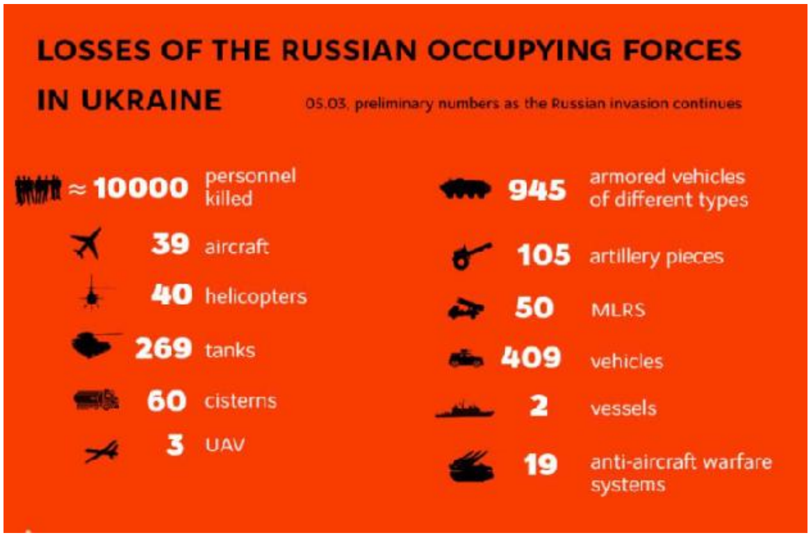
The rise of Artificial Intelligence (AI) has revolutionized the world in numerous ways, and its impact on warfare is no exception (Sheikh, 2022). The concept of Hybrid Warfare (HW) has emerged in recent years, which combines both conventional and unconventional methods of warfare (Royal, 2022). As per Raazia (2022),using AI in HW has added a new dimension to the war, which has significant implications for global security. This literature review aims to explore the impact of AI on HW, particularly in the context of the Russia-Ukraine war.

Hybrid Warfare:

HW is a form of warfare that combines conventional and unconventional methods, tactics, and technologies (Steingartner, 2021). It is a complex form of warfare that aims to achieve political objectives using military, economic, and informational means (Laruelle, 2021). Caliskan (2021) argued that using irregular forces, covert operations, propaganda, and disinformation campaigns characterizes it. The concept of hybrid warfare has gained significant attention in recent years due to its increasing use by state actors in various conflicts around the world (Thiele, 2021).

According to Janičatová (2021), the origins of hybrid warfare can be traced back to the Cold War era, when both the Soviet Union and the United States engaged in covert operations, propaganda, and disinformation campaigns to gain strategic advantages. However, as per Suchkov (2021),the term hybrid warfare was first used in the context of the 2006 Lebanon War between Israel and Hezbollah, where Hezbollah employed a combination of military, political, and media tactics to fight against the Israeli military.

Since then, Daniel (2021) narrated that various countries have used hybrid warfare in different conflicts, including the ongoing battle between Russia and Ukraine. The annexation of Crimea by Russia in 2014 marked the beginning of a hybrid war between the two countries, where Russia employed a combination of conventional military tactics and non-military measures, such as propaganda, cyberattacks, and economic pressure, to achieve its objectives (Tsygankov, 2021).



Source –(Ukarine War Bulletin, 2023)

According to the Ukraine War Bulletin (2023),Russia also faced losses in this war. Over 10,000 personnel are being killed in occupying areas of Ukraine. Similarly, their 39 aircraft, 40 helicopters, 269 tanks, and 3 UAVs are destroyed.

According to Brakto (2021), the use of hybrid warfare by state actors has been a cause of concern for the international community, as it challenges the traditional norms and principles of war. As per Käihkö (2021), the United Nations has recognized the need to address this issue and has established a working group to develop a shared understanding of hybrid threats and identify ways to manage them.

Various research studiesby Daniel (2021) and Suchkov (20210 have highlighted state actors' use of hybrid warfare tactics. A study by Dzutsati (2021) analyzed the conflict between Russia and

Ukraine and highlighted the role of hybrid warfare tactics in the conflict. The research foundthat Russia used information operations, cyberattacks, and economic pressure to achieve its objectives in the conflict.

Similarly, a study by Greg (2021) found the use of hybrid warfare tactics by non-state actors and highlighted the importance of strategic communication in countering these tactics. According to Erik Reichborn-Kjennerud and Patrick Cullen, the five main instruments of HW are military, political, economic, civil, and informational (MPECI) (Reichborn-Kjennerud & Cullen, 2016).

AI and Hybrid Warfare:

Artificial Intelligence (AI) is an umbrella term for computer systems designed to perform tasks that typically require human Intelligence, such as speech recognition, decision-making, and pattern recognition (Thiele, 2021). In recent years, AI has been used in various applications, including military operations, and has been linked to the concept of hybrid warfare (Pitman, 2022).

As per Hageback (2021),Hybrid Warfare (HW) is a form of warfare that combines conventional and unconventional tactics, including cyberattacks, psychological operations, and the use of proxy forces. According to Schmid (2021), the term hybrid warfare gained popularity after the 2014 Ukraine crisis, which involved a combination of conventional and unconventional tactics by Russia to annex Crimea and destabilize eastern Ukraine. The use of hybrid warfare tactics in this conflict demonstrated the ability of a state actor to employ a range of tactics to achieve strategic goals (Elonheimo, 2021).

The use of AI in hybrid warfare has been gaining attention in recent years. AI technologies such as machine learning and natural language processing are being used to analyze vast amounts of data and provide insights to decision-makers (Elonheimo, 2021). AI is also being used to develop autonomous weapons systems and enhance existing weapons systems' capabilities. The use of AI in hybrid warfare raises concerns about the potential for unintendedconsequences, such as escalating conflicts or using AI in unethical ways (Susnea, 2021).

There are few documented instances of AI being used in hybrid warfare. However, some research studies of AI are being used in military operations. For example, Royal (2022) found that during the 2014 conflict between Israel and Hamas, the Israeli military used AI to analyze social media data and identify potential targets. The use of AI in this conflict demonstrated the potential for AI to be used in military operations.

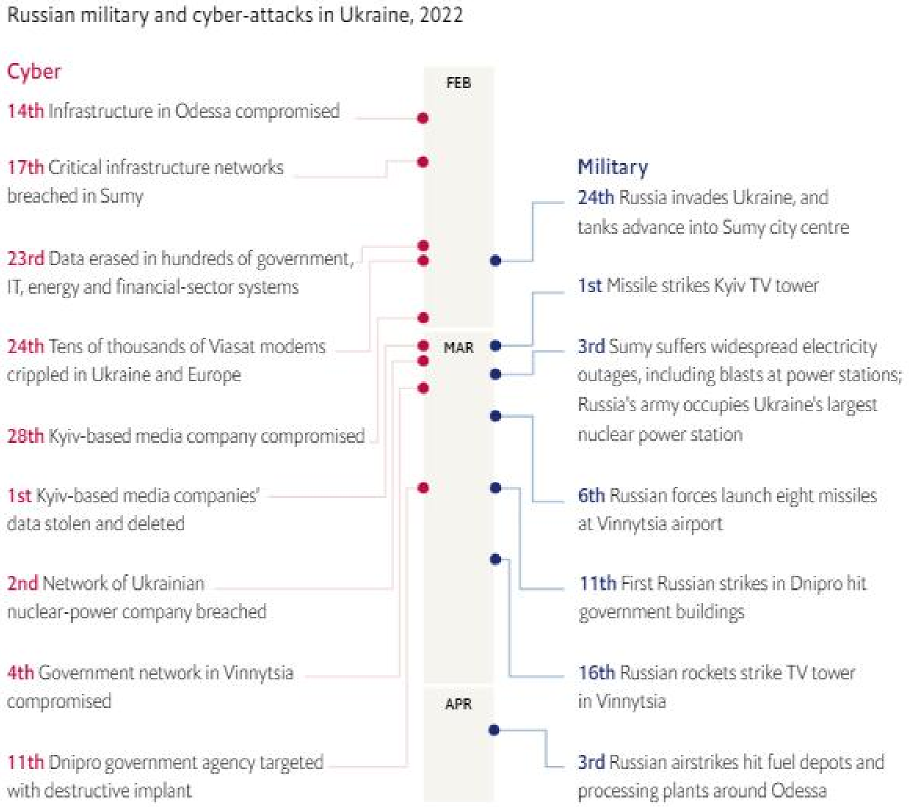
Research by Steingartner (2021) has also shown that countries are increasingly investing in AI for military purposes. This study found that AI is being developed for use in various military applications, including surveillance, targeting, and decision-making. The study also highlighted the potential for AI to be used in cyberattacks and developing autonomous weapons systems.

De Marchi (2021) argued that AI can transform HW by enabling faster decision-making, improving situational awareness, and enhancing the effectiveness of military operations. As per Libiseller (2023),AI can analyze vast amounts of data from various sources and provide real-time insights, which can assist in strategic decision-making. AI can also automate repetitive or dangerous tasks for humans, thereby reducing the risk to human lives. AI can assist in developing unmanned systems, which can perform various tasks, such as reconnaissance, surveillance, and target acquisition.

AI in the Russia-Ukraine War:

In the context of the Russia-Ukraine War, AI has been increasingly used by both state and non-state actors to gain a strategic advantage in the conflict. This literature review provides an overview of the role of AI in the Russia-Ukraine War, its background, and its impact on the different instruments of hybrid warfare.

According to Pandey (2023), the Russia-Ukraine conflict began in 2014 when Russia annexed Crimea, followed by an insurgency in the Donbass region of Ukraine. The conflict escalated into a hybrid war, featuring a combination of conventional and unconventional tactics, such as disinformation campaigns, cyber-attacks, propaganda, and the use of proxy forces. Hybrid warfare is defined as a strategy that blends conventional military operations with irregular tactics, such as propaganda, cyber-attacks, and covert operations, to achieve political objectives.



Russian military and cyber-attacks in Ukraine, 2022

Cyber

14th Infrastructure in Odessa compromised

17th Critical infrastructure networks breached in Sumy

23rd Data erased in hundreds of government, IT, energy and financial-sector systems

24th Tens of thousands of Viasat modems crippled in Ukraine and Europe

28th Kyiv-based media company compromised

1st Kyiv-based media companies' data stolen and deleted

2nd Network of Ukrainian nuclear-power company breached

4th Government network in Vinnytsia compromised

11th Dnipro government agency targeted with destructive implant

Military

24th Russia invades Ukraine, and tanks advance into Sumy city centre

1st Missile strikes Kyiv TV tower

3rd Sumy suffers widespread electricity outages, including blasts at power stations; Russia's army occupies Ukraine's largest nuclear power station

6th Russian forces launch eight missiles at Vinnytsia airport

11th First Russian strikes in Dnipro hit government buildings

16th Russian rockets strike TV tower in Vinnytsia

3rd Russian airstrikes hit fuel depots and processing plants around Odessa

Source (Economist, 2023)

According to the above statistics and figures, there were several cyber attacks and military attacks conducted by the Russian forces in Ukraine only in the month of February, March, and April 2023. The above figureindicates that the Russian troops in Ukraine conducted total of 9 cyberattacks in these three months. Similarly, the above figure also shows that Russian forces in Ukraine conducted a total of seven military attacks during these three months.

Russell (2023) argued that using AI in the Russia-Ukraine War has impacted the instruments of hybrid warfare, especially in the military and informational domains. In the military domain, AI has provided a significant advantage in surveillance, target selection, and battle simulation. AI-powered drones have enabled more precise targeting, reduced collateral damage, and minimized the risk to human operators. In the informational domain, AI has generated fake news and disinformation campaigns, creating confusion and sowing distrust among the opposing forces. The use of AI in propaganda and disinformation campaigns has also increased the effectiveness of psychological operations, allowing the state and non-state actors to influence public opinion and shape the narrative of the conflict (Anghel, 2023). The hybrid warfare model proposed by Erik Reichborn-Kjennerud and Patrick Cullen, which is based on five instruments: military, political, economic, civil, and informational (MPECI), provides a valuable framework for analyzing the impact of AI in the Russia-Ukraine War (Yan, 2020).

The findings of Shen et al. (2023) indicate that AI has played a significant role in the Russia-Ukraine War, both in the military and informational instruments of hybrid warfare. In the military domain, AI has been used for surveillance, target selection, and battle simulation. Both sides have deployed AI-powered drones for intelligence gathering and targeted strikes. AI algorithms have also been used to analyze satellite imagery to identify enemy positions and activities. In the informational domain, AI has been used for disinformation campaigns, fake news generation, and social media manipulation (AlQershi, 2023). AI algorithms have been used to create deepfake videos and photos to spread false information and create confusion among the opposing forces.

Military: AI has been used to improve the effectiveness of military operations in the Russia-Ukraine war. A study conducted by Zhao (2023) found that the use of unmanned systems, such as drones, has increased. These unmanned systems can provide real-time information about enemy positions, assisting in planning and executing military operations. AI can also assist in developing autonomous weapon systems, which can perform tasks without human intervention.

According to a study by Huang (2023),the Russian military has been developing AI-based weapons for use in the Ukraine conflict. These weapons include drones, uncrewed ground vehicles, and autonomous underwater vehicles. These AI-powered weapons systems are designed to enhance situational awareness, provide intelligence, surveillance, and reconnaissance (ISR) capabilities, and enable enemy forces targeting. These systems are also equipped with advanced sensors and algorithms that can quickly process large amounts of data, providing real-time information to military commanders.

In addition to AI-powered weapons systems, the Russian military has also been using AI to analyze data gathered from various sources, including social media, to gain insights into the movements and activities of Ukrainian forces. This information is used to develop a more accurate picture of the battlefield and to help plan military operations.

According to a study by Vyas (2023), the Russian military has been using AI-powered unmanned aerial vehicles (UAVs) to conduct reconnaissance and surveillance in the conflict. The research also notes that Russian-backed separatists have been using drones equipped with AI-powered targeting systems to attack Ukrainian forces.

Another research by Neik et al., (2023) highlights the growing use of AI in the Russian military, noting that the country is investing heavily in developing advanced technologies, including AI. The study suggests that the Russian military will likely continue investing in these technologies, which could have significant implications for future conflicts.

Political: AI has been used in the Russia-Ukraine war to influence public opinion and shape the political narrative. As per Rose (2023), the use of bots and automated accounts on social media platforms has been observed, which can create the impression of widespread support for a particular view or opinion. AI algorithms can also analyze public sentiment and adjust messaging to increase the effectiveness of propaganda campaigns.

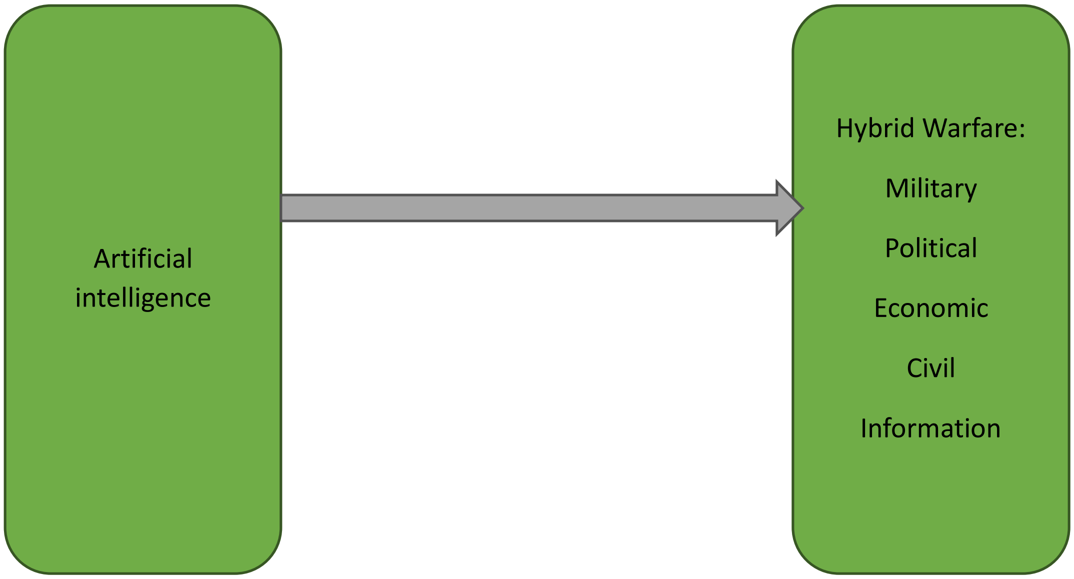
Economic: The use of AI in the monetary instrument of HW has been limited in the Russia-Ukraine war. Xu et al. (2023) state that AI can potentially disrupt critical infrastructure and cause economic damage. Cyber-attacks on banking systems, energy grids, and other critical infrastructure can be carried out using AI-powered tools.

Civil: AI can be used to identify and target vulnerable populations in the civil instrument of HW. A study by Amar (2023) found that AI algorithms can analyze social media activity to identify individuals susceptible to extremist ideologies. This information can then be used to target individuals with propaganda campaigns or to recruit them into extremist groups.

Informational: The use of AI in the informative instrument of HW has been widespread in the Russia-Ukraine war. Malhotra (2023) found that disinformation campaigns have been carried out using AI-powered bots, which can create and disseminate fake news stories. AI algorithms can also be used to create deep fakes, which can spread false information.

Model

The use of AI in propaganda and disinformation campaigns has also increased the effectiveness of psychological operations, allowing the state and non-state actors to influence public opinion and shape the narrative of the conflict. The hybrid warfare model proposed by Erik Reichborn-Kjennerud and Patrick Cullen, which is based on five instruments: military, political, economic, civil, and informational (MPECI), provides a valuable framework for analyzing the impact of AI in the Russia-Ukraine War (Yan, 2020).



MPECI Model developed by Erik Reichborn-Kjennerud and Patrick Cullen.

Source (Yan, 2020)

Discussion

AI has played a significant role in the Russia-Ukraine War, both in hybrid warfare's military and informational instruments (Xu, 2023). In the military domain, AI has been used for reconnaissance, target selection, and battle simulation (Rose, 2023). Both sides have deployed AI-powered drones for intelligence gathering and targeted strikes (Neik, 2023). AI algorithms have also analyzed satellite imagery to identify enemy positions and activities (Amar, 2023). In the informational domain, AI has been used for disinformation campaigns, fake news generation, and social media manipulation (Malhotra, 2023). AI algorithms have been used to create deepfake videos and photos to spread false information and create confusion among the opposing forces.

Military: AI has been used to improve the effectiveness of military operations in the Russia-Ukraine war. Russell (2023) found that the use of unmanned systems, such as drones, has increased. These unmanned systems can provide real-time information about enemy positions, which can assist in planning and executing military operations. AI can also assist in developing autonomous weapon systems, which can perform tasks without human intervention.

According to a study by Anghel (2023), the Russian military has been developing AI-based weapons for use in the Ukraine conflict. These weapons include drones, uncrewed ground vehicles, and autonomous underwater vehicles. Moreover, as per Shen (2023), these AI-powered weapons systems are designed to enhance situational awareness, provide intelligence, surveillance, and reconnaissance (ISR) capabilities, and enable enemy forces targeting. These systems are also equipped with advanced sensors and algorithms that can quickly process large amounts of data, providing real-time information to military commanders.

Zhao (2023) also found that AI-powered weapons systems, the Russian military, have also been using AI to analyze data gathered from various sources, including social media, to gain insights into the movements and activities of Ukrainian forces. This information is used to develop a more accurate picture of the battlefield and to help plan military operations.

According to research by Wadhwani (2023),the Russian military has been using AI-powered uncrewed aerial vehicles (UAVs) to conduct reconnaissance and surveillance in the conflict. The report also notes that Russian-backed separatists have been using drones equipped with AI-powered targeting systems to attack Ukrainian forces.

Another research by Xu (2023) highlights the growing use of AI in the Russian military, noting that the country is investing heavily in developing advanced technologies, including AI. The report suggests that the Russian military will likely continue investing in these technologies, which could have significant implications for future conflicts.

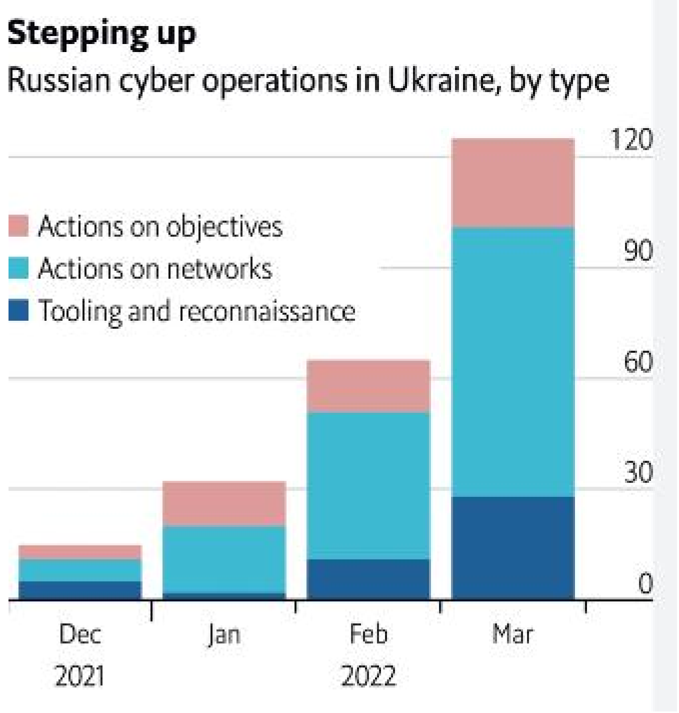
Political: AI has been used in the Russia-Ukraine war to influence public opinion and shape the political narrative. According to Ahmed (2022),AI has been used by the Russian government to control the media narrative and spread propaganda to manipulate public opinion. This section will review the existing literature on how AI is used in the Russia-Ukraine War's political aspects.

One way AI is used in the conflict's political aspects is through social media manipulation. A study by Alyukov (2022)indicates that the Russian government was using Twitter and other social media platforms to spread disinformation and propaganda during the conflict. They found that bots and trolls were being used to amplify pro-Russian sentiment and to discredit the Ukrainian government. Additionally, the report found that the Russian government was using AI to generate content and manipulate images to support their narrative.

Another research by Hurak (2022) found that AI is being used in the political aspects of conflict through surveillance. The Russian government has been using facial recognition software to identify protesters and dissidents, as well as to track the movements of Ukrainian soldiers. This has allowed them to monitor and control public dissent and to gain an advantage on the battlefield.

Jagtap (2022) also found that AI is being used to automate decision-making processes in the Russian government. This study further found that the Russian government was using AI to make military strategy and foreign policy decisions. This has allowed them to make decisions quickly and efficiently, giving them an advantage over their adversaries. The use of bots and automated accounts on social media platforms has been observed, which can create the impression of widespread support for a particular view or opinion. AI algorithms can also analyze public sentiment and adjust messaging to increase the effectiveness of propaganda campaigns.

Economic: The use of AI in the monetary instrument of HW has been limited in the Russia-Ukraine war. As per Susnea (2021), AI can potentially be used to disrupt critical infrastructure and cause economic damage. Cyber-attacks on banking systems, energy grids, and other critical infrastructure can be carried out using AI-powered tools.



Source (Economist, 2023)

The above statistics indicate that Russia has increased cyber-attacks in 2022. These were significantly increased in the month of March. The figure illustrates that there are over 120 cyber-attacks on actions and objectives by Russia in Ukraine.

Another study by Crocker (2022) found that the way AI is being used in the economic aspects of conflict is through the use of cyber-attacks. In 2015, Ukrainian power plants were targeted in a cyber-attack that caused widespread power outages. It is believed that Russian hackers used AI and machine learning algorithms to infiltrate the power grid and cause the outages. This incident highlights the potential for AI to be used in economic warfare through cyber-attacks on critical infrastructure.

Moreover, Willett (2022) argued that AI is also being used in the logistics of the conflict. The Russian military has reportedly been using AI-powered logistics systems to optimize the movement of troops and supplies. These systems can analyze weather conditions, terrain, and other factors to determine the most efficient routes for troops and supplies.

There is also evidence in the research by Alam (2022) that AI is being used in the economic warfare tactics of information warfare. Russian state-sponsored media outlets have been using AI algorithms to create and disseminate propaganda targeted at Ukrainian civilians and soldiers. This propaganda is designed to undermine the Ukrainian government and military and sow discord among the population.

Civil: AI can be used to identify and target vulnerable populations in the civil instrument of HW. A study by Loskutov (2022) indicates that AI algorithms can analyze social media activity to identify individuals susceptible to extremist ideologies. This information can then be used to target individuals with propaganda campaigns or to recruit them into extremist groups.

Pandey (2023) found that AI significantly impacts the civil aspect of hybrid warfare in the Russia-Ukraine conflict, and non-state actors mostly use it to create a disinformation campaign to manipulate the opinions and beliefs of the population. AI-powered bots and algorithms can influence people's opinions, suppress opposing views, and promote misinformation to create an environment of chaos and instability.

According to a study by Prakasa (2022), the pro-Russian separatists and Russian state actors used AI-based disinformation campaigns to manipulate the Ukrainian population during the 2014 conflict. The study stated that Russia used a combination of AI-based bots, cyber-attacks, and online propaganda to influence the Ukrainian people, creating an environment of instability and weakening the Ukrainian government's legitimacy.

Similarly, research by Uwishema (2022) found that AI-based bots and algorithms are used to manipulate public opinion in the Russia-Ukraine conflict. A report by the Atlantic Council's Digital Forensic Research Lab (DFRLab) stated that Russian-based bots used AI algorithms to promote anti-Ukrainian propaganda on social media platforms like Twitter, Facebook, and Instagram. The study also revealed that Russian-based organizations and individuals controlled these bots.

A research paper by Jagtap (2022) has also highlighted the role of AI in the civil aspect of hybrid warfare in the Russia-Ukraine conflict. A study by Xu (2023) stated that Russia used AI-based disinformation campaigns to create a narrative that supported Russian military intervention in Ukraine. The study further noted that these disinformation campaigns created a sense of instability in Ukraine, which increased the chances of successful Russian intervention.

Informational: The use of AI in the informative instrument of HW has been widespread in the Russia-Ukraine war. As per Willett (2022), disinformation campaigns have been carried out using AI-powered bots, which can create and disseminate fake news stories. AI algorithms can also be used to create deep fakes, which can be used to spread false information.

According to Ha (2022), in the context of the Russia-Ukraine war, AI is being used to gather and analyze vast amounts of data to create sophisticated disinformation campaigns, manipulate public opinion, and destabilize target countries. The Russian Federation is using AI to advance its strategic communications and propaganda efforts, create fake news stories, and develop deepfakes to manipulate public perception and spread false information (Pohl, 2022). Additionally, the Russian military is utilizing AI in the battlefield to analyze and interpret intelligence information, track and target enemy movements, and operate uncrewed aerial vehicles.

A study by Pohl (2022) states that the Russian Federation is using AI to spread disinformation and propaganda, which has fueled the conflict in Ukraine. The research highlights how AI is being used to target and manipulate vulnerable populations through social media, messaging apps, and online forums. It also notes that using AI in hybrid warfare can have severe consequences for human rights, including freedom of expression, access to information, and the right to participate in public life.

Another study by Abakeh (2022) argued the use of AI in hybrid warfare, specifically in the information domain. The global consulting firm Deloitte has published several reports on the topic, highlighting the importance of AI in understanding the tactics and strategies used in hybrid warfare. The research also emphasizes the need for countries to develop their capabilities in AI to counter these emerging threats.

A research study by Zhao (2023) has explored the use of AI in hybrid warfare and its implications for national security. Research by Johnston (2021) analyzed the Russian Federation's use of AI in Ukraine's disinformation campaigns and propaganda efforts. They argue that AI is being used to undermine democratic institutions, fuel ethnic tensions, and destabilize target countries.

Conclusion

In conclusion, this research has explored the impact of Artificial Intelligence (AI) on hybrid warfare, with a specific focus on the Russia-Ukraine war. Applying the hybrid warfare model proposed by Erik Reichborn-Kjennerud and Patrick Cullen, the research has analyzed how AI impacts the military, political, economic, civil, and informational instruments of hybrid warfare.

The findings of this research indicate that AI is playing an increasingly important role in hybrid warfare, particularly in the informational aspect. State and non-state actors use AI to spread propaganda, influence public opinion, and conduct cyber-attacks. Moreover, AI is also being used to improve military decision-making, target selection, and intelligence gathering.

Implications

The implications of these findings are significant, not only for state and non-state actors but also for the international community. The use of AI in hybrid warfare poses a significant challenge to the existing legal and regulatory frameworks governing warfare. Furthermore, the increasing use of AI in hybrid warfare has the potential to undermine the integrity of democratic processes and institutions.

Overall, this research highlights the need for policymakers, military strategists, and the international community to develop a comprehensive understanding of the implications of AI in hybrid warfare. It also calls for a concerted effort to establish appropriate regulatory frameworks to govern the use of AI in warfare and ensure that it is used responsibly and ethically.

Limitations

The research is focused on the case of the Russia-Ukraine war, and the findings may not be applicable to other contexts.The research is based on a literature review and may not capture the full scope of AI use in hybrid warfare in the Russia-Ukraine conflict.The research is limited to publicly available information and may not capture classified or undisclosed uses of AI in hybrid warfare.

Future studies

Future studies may conduct case studies on the use of AI in hybrid warfare in other conflicts to understand how AI impacts the instruments of hybrid warfare in different contexts. Future studies can also conduct empirical studies to assess the effectiveness of AI in hybrid warfare and its impact on military, political, economic, civil, and informational instruments of power. Moreover, future studies can also investigate the ethical implications of AI use in hybrid warfare and its impact on civilians and non-combatants.

References

Abakah, E. J. A., Adeabah, D., Tiwari, A. K., & Abdullah, M. (2022). Analyzing the Effect of Public Sentiment Towards Economic Sanctions News during Russia-Ukraine Conflict on Blockchain Market and Fintech Industry. *Available at SSRN 4359071*.

Ahmed, S., Hasan, M. M., & Kamal, M. R. (2022). Russia–Ukraine crisis: The effects on the European stock market. *European Financial Management*.

Alam, M. K., Tabash, M. I., Billah, M., Kumar, S., & Anagreh, S. (2022). The impacts of the Russia–Ukraine invasion on global markets and commodities: a dynamic connectedness among G7 and BRIC markets. *Journal of Risk and Financial Management*, *15*(8), 352.

AlQershi, N., Saufi, R. B. A., Ismail, N. A., Mohamad, M. R. B., Ramayah, T., Muhammad, N. M. N., & Yusoff, M. N. H. B. (2023). The moderating role of market turbulence beyond the Covid-19 pandemic and Russia-Ukraine crisis on the relationship between intellectual capital and business sustainability. *Technological Forecasting and Social Change*, *186*, 122081.

Alyukov, M. (2022). Making sense of the news in an authoritarian regime: Russian television viewers' reception of the Russia–Ukraine conflict. *Europe-Asia Studies*, *74*(3), 337-359.

Amar, A. B., Bouattour, M., Bellalah, M., & Goutte, S. (2023). Shift contagion and minimum causal intensity portfolio during the COVID-19 and the ongoing Russia-Ukraine conflict. *Finance Research Letters*, 103853.

Anghel, V., & Jones, E. (2023). Is Europe really forged through crisis? Pandemic EU and the Russia–Ukraine war. *Journal of European Public Policy*, *30*(4), 766-786.

Armitage, R. (2022). Battlefronts in Ukraine: Russian invasion and COVID-19. *British Journal of General Practice*, *72*(720), 334-334.

Baker, M. S., Baker, J., & Burkle Jr, F. M. (2023). Russia's Hybrid Warfare in Ukraine Threatens Both Healthcare & Health Protections Provided by International Law. *Annals of global health*, *89*(1).

Bratko, A., Zaharchuk, D., & Zolka, V. (2021). Hybrid warfare–a threat to the national security of the state. *Revista de Estudios en Seguridad Internacional*, *7*(1), 147-160.

Burkle, F. M., Goniewicz, K., & Khorram-Manesh, A. (2022). Bastardizing peacekeeping and the birth of hybrid warfare. *Prehospital and disaster medicine*, *37*(2), 147-149.

Caliskan, M., & Liégeois, M. (2021). The concept of 'hybrid warfare'undermines NATO's strategic thinking: insights from interviews with NATO officials. *Small wars & insurgencies*, *32*(2), 295-319.

Clark, M. (2020). *Russian hybrid warfare*. Washington, DC: Institute for the Study of War.

Crocker, C. A. (2022). Endings and Surprises of the Russia–Ukraine War. *Survival*, *64*(5), 183-192.

Cusumano, E., & Corbe, M. (Eds.). (2018). *A civil-military response to hybrid threats*. Cham, Switzerland: Palgrave Macmillan.

Daniel, J., & Eberle, J. (2021). Speaking of hybrid warfare: Multiple narratives and differing expertise in the 'hybrid warfare'debate in Czechia. *Cooperation and Conflict*, *56*(4), 432-453.

de Marchi, J. A., Sharp, J., Melrose, J., Madahar, B., Kurth, F., Lange, D. S., ... & Tanik, G. O. (2021). Robustness of Artificial Intelligence for Hybrid Warfare.

Dzutsati, V. (2021). Geographies of hybrid war: rebellion and foreign intervention in Ukraine. *Small Wars & Insurgencies*, *32*(3), 441-468.

Economist., (2023). Russia seems to be co-ordinating cyber-attacks with its military campaign. *The Economist*. Retrieved from https://www.economist.com/graphic-detail/2022/05/10/russia-seems-to-be-co-ordinating-cyber-attacks-with-its-military-campaign

Elonheimo, T. (2021). Comprehensive Security Approach in Response to Russian Hybrid Warfare. *Strategic Studies Quarterly*, *15*(3), 113-137.

Gasztold, A., & Gasztold, P. (2022). The Polish Counterterrorism System and Hybrid Warfare Threats. *Terrorism and political violence*, *34*(6), 1259-1276.

Greg, S. (2021). Operational implications and effects of informational and political dimensions of western hybrid warfare. *Вестник Московского государственного областного университета*, (3), 106-116.

Ha, L. T. (2022). Dynamic interlinkages between the crude oil and gold and stock during Russia-Ukraine War: evidence from an extended TVP-VAR analysis. *Environmental Science and Pollution Research*, 1-14.

Hageback, N., & Hedblom, D. (2021). *AI for Digital Warfare*. CRC Press.

Hird, K. (2023). Russian Offensive Campaign Assessment, March 15, 2023-Karolina Hird, Kateryna Stepanenko, Grace Mappes, Nicole Wolkov, Layne Philipson.

Huang, M., Shao, W., & Wang, J. (2023). Correlations between the crude oil market and capital markets under the Russia–Ukraine conflict: A perspective of crude oil importing and exporting countries. *Resources Policy*, *80*, 103233.

Hurak, I., & D'Anieri, P. (2022). The Evolution of Russian Political Tactics in Ukraine. *Problems of Post-Communism*, *69*(2), 121-132.

Jagtap, S., Trollman, H., Trollman, F., Garcia-Garcia, G., Parra-López, C., Duong, L., ... & Afy-Shararah, M. (2022). The Russia-Ukraine conflict: Its implications for the global food supply chains. *Foods*, *11*(14), 2098.

Janičatová, S., & Mlejnková, P. (2021). The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities. *Contemporary security policy*, *42*(3), 312-344.

Johnston, B. (2021). Social media: The new intelligence collection platforms. *United Service*, *72*(4), 15-16.

Käihkö, I. (2021). The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession. *The US Army War College Quarterly: Parameters*, *51*(3), 11.

Khorram-Manesh, A., & Burkle, F. M. (2022). Civilian population victimization: a systematic review comparing humanitarian and health outcomes in conventional and hybrid warfare. *Disaster medicine and public health preparedness*, 1-30.

Khorram-Manesh, A., & Burkle, F. M. (2022). Civilian population victimization: a systematic review comparing humanitarian and health outcomes in conventional and hybrid warfare. *Disaster medicine and public health preparedness*, 1-30.

Kricorian, K., Khoshnood, K., & Chekijian, S. (2022). Hybrid warfare and public health: Conflicts in Ukraine and Nagorno-Karabakh raise the alarm. *Public Health in Practice*, *4*, 100342.

Kurapov, A., Pavlenko, V., Drozdov, A., Bezliudna, V., Reznik, A., & Isralowitz, R. (2023). Toward an understanding of the Russian-Ukrainian war impact on university students and personnel. *Journal of Loss and Trauma*, *28*(2), 167-174.

Laruelle, M., & Limonier, K. (2021). Beyond "hybrid warfare": a digital exploration of Russia's entrepreneurs of influence. *Post-Soviet Affairs*, *37*(4), 318-335.

Libiseller, C. (2023). 'Hybrid warfare'as an academic fashion. *Journal of Strategic Studies*, 1-23.

Loskutov, O. A., & Pylypenko, M. M. (2022). The courage of Ukrainian hospitals and intensive care units in the first months of the Russia–Ukraine war. *Intensive Care Medicine*, *48*(6), 790-792.

Malhotra, G., Yadav, M. P., Tandon, P., & Sinha, N. (2023). An investigation on dynamic connectedness of commodity market with financial market during the Russia–Ukraine invasion. *Benchmarking: An International Journal*.

Mattingsdal, J., Espevik, R., Johnsen, B. H., & Hystad, S. (2023). Exploring Why Police and Military Commanders Do What They Do: An Empirical Analysis of Decision-Making in Hybrid Warfare. *Armed Forces & Society*, 0095327X231160711.

Mbah, R. E., & Wasum, D. F. (2022). Russian-Ukraine 2022 War: A review of the economic impact of Russian-Ukraine crisis on the USA, UK, Canada, and Europe. *Advances in Social Sciences Research Journal*, *9*(3), 144-153.

Morejón-Llamas, N., Martín-Ramallal, P., & Micaletto-Belda, J. P. (2022). Twitter content curation as an antidote to hybrid warfare during Russia's invasion of Ukraine. *Profesional de la información*, *31*(3).

Mumford, A., & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, *8*(2), 192-206.

Muradov, I. (2022). The Russian hybrid warfare: the cases of Ukraine and Georgia. *Defence studies*, *22*(2), 168-191.

Muradov, I. (2022). The Russian hybrid warfare: the cases of Ukraine and Georgia. *Defence studies*, *22*(2), 168-191.

Neik, T. X., Siddique, K. H., Song, B. K., Mayes, S., Edwards, D., Batley, J., ... & Massawe, F. (2023). Diversifying agrifood systems to ensure global food security following the Russia-Ukraine crisis. *Frontiers in Sustainable Food Systems*, *7*, 127.

Ociepa-Kicińska, E., & Gorzałczyńska-Koczkodaj, M. (2022). Forms of Aid Provided to Refugees of the 2022 Russia–Ukraine War: The Case of Poland. *International journal of environmental research and public health*, *19*(12), 7085.

Pandey, D. K., & Kumar, R. (2023). Russia-Ukraine War and the global tourism sector: A 13-day tale. *Current Issues in Tourism*, *26*(5), 692-700.

Patel, S. S., & Erickson, T. B. (2022). The new humanitarian crisis in Ukraine: Coping with the public health impact of hybrid warfare, mass migration, and mental health trauma. *Disaster medicine and public health preparedness*, 1-2.

Pitman, L. (2022). Perfect Strangers: Legal and Ethical Aspects of AI in Hybrid Warfare. *Practical Applications of Advanced Technologies for Enhancing Security and Defense Capabilities: Perspectives and Challenges for the Western Balkans*, *155*, 32.

Pohl, J., Seiler, M. V., Assenmacher, D., & 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*.

Prakasa, S. U. W., Wijayanti, A., Hariri, A., & Yustitianingtyas, L. (2022). The Effect of Russia--Ukraine War on International Aviation Sectors. *KnE Social Sciences*, 572-581.

Raazia, I., Butt, M. A. J., & Rafaqat, I. (2022). Conceptualizing Hybrid Warfare: India's Tactics Confronting Pakistan's Security. *Journal of the Research Society of Pakistan*, *59*(3), 104.

Rose, A., Chen, Z., & Wei, D. (2023). The economic impacts of Russia–Ukraine War export disruptions of grain commodities. *Applied Economic Perspectives and Policy*.

Royal, N. L. R. (2022). Robustness of Artificial Intelligence for Hybrid Warfare.

Royal, N. L. R. (2022). Robustness of Artificial Intelligence for Hybrid Warfare.

Russell, S. (2023). AI weapons: Russia's war in Ukraine shows why the world must enact a ban. *Nature*, *614*(7949), 620-623.

Schmid, J. (2021). Introduction to Hybrid Warfare–A Framework for comprehensive Analysis. *Hybrid Warfare: Future and Technologies*, 11-32.

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*.

Shiekh, H. (2022). AI as a Tool of Hybrid Warfare: Challenges and Responses. *Journal of Information Warfare*, *21*(2), 36-49.

Solmaz, T. (2022).' Hybrid Warfare'One Term, Many Meanings. *Small Wars Journal*.

Steingartner, W., & Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. *Acta Polytechnica Hungarica*, *18*(3), 25-45.

Steingartner, W., & Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. *Acta Polytechnica Hungarica*, *18*(3), 25-45.

Suchkov, M. A. (2021). Whose hybrid warfare? How 'the hybrid warfare'concept shapes Russian discourse, military, and political practice. *Small Wars & Insurgencies*, *32*(3), 415-440.

Șușnea, E., & Ionuț-Cosmin, B. U. Ț. Ă. (2021). ARTIFICIAL INTELLIGENCE IN HYBRID WARFARE: A LITERATURE REVIEW AND CLASSIFICATION. *STRATEGIES XXI-Security and Defense Faculty*, *17*(1), 294-302.

Thiele, R. (Ed.). (2021). *Hybrid Warfare: Future and Technologies*. Springer Nature.

Tsygankov, A. P., Tsygankov, P. A., & Gonzales, H. (2021). Putin's "global hybrid war": US experts, Russia, and the Atlantic Council. *Russia in Global Affairs*, *19*(1), 146-172.

Ukarine War Bulletin., (2023). Ukraine: war bulletin: Russian aggression against Ukraine as of march 5, 14.00 CET. *Small Wars Journal*. Retrieved from https://smallwarsjournal.com/blog/ukraine-war-bulletin-russian-aggression-against-ukraine-march-5-1400-cet

Umbach, F. (2022). Russia's cyber fog in the Ukraine war. *GIS Reports*. Retrieved from https://www.gisreportsonline.com/r/russia-cyber/. Retrieved on March 20, 2023

Uwishema, O., Sujanamulk, B., Abbass, M., Fawaz, R., Javed, A., Aboudib, K., ... & Onyeaka, H. (2022). Russia-Ukraine conflict and COVID-19: a double burden for Ukraine's healthcare system and a concern for global citizens. *Postgraduate Medical Journal*, *98*(1162), 569-571.

Vorbrugg, A., & Bluwstein, J. (2022). Making sense of (the Russian war in) Ukraine: On the politics of knowledge and expertise. *Political geography*, 102700.

Vyas, P., Vyas, G., & Dhiman, G. (2023). RUemo—The Classification Framework for Russia-Ukraine War-Related Societal Emotions on Twitter through Machine Learning. *Algorithms*, *16*(2), 69.

Wadhwani, G. K., Varshney, P. K., Gupta, A., & Kumar, S. (2023). Sentiment Analysis and Comprehensive Evaluation of Supervised Machine Learning Models Using Twitter Data on Russia–Ukraine War. *SN Computer Science*, *4*(4), 346.

Wells, J. S. (2022). Preparing for hybrid warfare and cyberattacks on health services' digital infrastructure: What nurse managers need to know. *Journal of Nursing Management*, *30*(6), 2000-2004.

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival*, *64*(5), 7-26.

Xu, W., Pavlova, I., Chen, X., Petrytsa, P., Graf-Vlachy, L., & Zhang, S. X. (2023). Mental health symptoms and coping strategies among Ukrainians during the Russia-Ukraine war in March 2022. *International journal of social psychiatry*, 00207640221143919.

Xu, W., Pavlova, I., Chen, X., Petrytsa, P., Graf-Vlachy, L., & Zhang, S. X. (2023). Mental health symptoms and coping strategies among Ukrainians during the Russia-Ukraine war in March 2022. *International journal of social psychiatry*, 00207640221143919.

Yan, G. (2020). The impact of Artificial Intelligence on hybrid warfare. *Small Wars & Insurgencies*, *31*(4), 898-917.

Zhao, B., Ren, W., Zhu, Y., & Zhang, H. (2023). Manufacturing conflict or advocating peace? a study of social bots agenda building in the twitter discussion of the Russia-Ukraine war. *Journal of Information Technology & Politics*, 1-19.