An Analytical Framework of Contemporary Hybrid Warfare: Lessons Learned from the Russia–Ukraine War

Аналітична рамка сучасної гібридної війни: уроки, отримані з російсько-української війни

Khayal Iskandarov
Corresponding author: PhD in National Security and Military Sciences, e-mail: xayal1333@gmail.com, ORCID ID: https://orcid.org/0000-0001-8975-6530

Elmeddin Aliyev
e-mail: xayal1333@gmail.com, ORCID ID: https://orcid.org/0009-0004-7830-2364

Azerbaijan Technical University, Baku, Azerbaijan

Хаял Іскандаров
Corresponding author: к. наук з національної безпеки та військових наук, e-mail: xayal1333@gmail.com, ORCID ID: https://orcid.org/0000-0001-8975-6530

Елмеддін Алієв
e-mail: xayal1333@gmail.com, ORCID ID: https://orcid.org/0009-0004-7830-2364

Азербайджанський технічний університет, Баку, Азербайджан

Received: April 7, 2026 | Revised: April 21, 2026 | Accepted: April 30, 2026

UDC 355.4:355.01:004.056

DOI: https://doi.org/10.33445/sds.2026.16.2.1

Purpose. To conceptualize the operational characteristics of hybrid warfare by examining the Russia–Ukraine war as an empirical case study.

Method: Comparative analysis, and synthesis.

Findings. The empirical analysis shows that hybrid warfare is a systematic integration of non-military and military instruments within a multi-domain strategy. Russia combined cyber operations, information warfare, intelligence activities, economic pressure, psychological operations, and conventional forces to shape the operational environment. Non-military asymmetric measures constituted the initial and prolonged phase (2014–2022), aimed at undermining infrastructure, public trust, and international narratives; however, Ukraine's cyber resilience prevented systemic collapse. Disinformation and psychological operations targeted political and military leadership to create uncertainty, but their effectiveness was limited by rapid fact-checking and strategic communication. Hybrid warfare also exploits institutional vulnerabilities (corruption, bribery, intimidation), yet anti-corruption measures and reforms helped contain these risks. Propaganda and bot networks were used to weaken social cohesion; however, counter-disinformation mechanisms helped maintain public trust. Further escalation involves more overt pressure through air, maritime, and proxy instruments. Intelligence operations and troop buildups preceded the invasion, but early mobilization and international cooperation reduced the element of surprise. Ultimately, hybrid warfare evolves into a multi-domain campaign involving missile strikes, electronic warfare, and unmanned systems, which Ukraine countered through layered air defense, interception technologies, and enhanced infrastructure resilience. Thus, hybrid warfare represents a continuum of integrated instruments of influence, the effectiveness of which can be limited by strong institutional capacity, cyber resilience, and international support.

Theoretical implications. The findings refine the conceptual understanding of hybrid warfare within security studies.

Practical implications. The results are relevant for policymakers and defense institutions addressing hybrid threats.

Paper type. Theoretical.

Key words: Hybrid Warfare, Russia–Ukraine War, Cyber Warfare, Information Warfare, Multi-Domain Operations, Strategic Deception, State Resilience.

Мета дослідження. Концептуалізувати операційні характеристики гібридної війни шляхом аналізу російсько-української війни як емпіричного кейсу.

Метод дослідження. Порівняльний аналіз і синтез.

Результати дослідження. Емпіричний аналіз показує, що гібридна війна є системною інтеграцією немілітарних і військових інструментів у межах багатодоменної стратегії. Росія поєднувала кібероперації, інформаційну війну, розвідку, економічний тиск, психологічні операції та конвенційні сили для формування операційного середовища. Немілітарні асиметричні заходи становили початкову і тривалу фазу (2014–2022), спрямовану на підрив інфраструктури, довіри та міжнародних наративів, однак кіберстійкість України не допустила системного колапсу. Дезінформаційні та психологічні операції були орієнтовані на політичне і військове керівництво з метою створення невизначеності, проте їх ефективність обмежувалась швидким фактчекінгом і стратегічними комунікаціями. Гібридна війна також експлуатує інституційні вразливості (корупція, підкуп, залякування), але антикорупційні заходи та реформи сприяли їх стримуванню. Пропаганда і бот-мережі застосовувалися для підриву соціальної згуртованості, однак механізми протидії дезінформації дозволили зберегти суспільну довіру. Подальша ескалація передбачає відкриті форми тиску через повітряні, морські та проксі-інструменти. Розвідувальні операції і концентрація військ передували вторгненню, але рання мобілізація та міжнародна співпраця зменшили ефект несподіванки. У підсумку гібридна війна трансформується у багатодоменну кампанію з використанням ракетних ударів, РЕБ і безпілотних систем, яким Україна протидіє через багаторівневу ППО, перехоплення та підвищення стійкості інфраструктури. Отже, гібридна війна є континуумом інтегрованих інструментів впливу, ефективність яких може бути обмежена за умов високої інституційної спроможності, кіберстійкості та міжнародної підтримки.

Теоретична цінність дослідження. Результати уточнюють концептуальне розуміння гібридної війни в межах безпекових студій.

Практична цінність дослідження. Результати корисні для формування політик протидії гібридним загрозам.

Тип статті. Теоретична.

Ключові слова: Гібридна війна, російсько-українська війна, кібернетична війна, інформаційна війна, багатодоменні операції, стратегічна дезінформація, стійкість держави.

Introduction

The term “hybrid warfare” has dominated academic and military-strategic discussions on modern and future conflicts since the 2006 Lebanon War. It has been widely adopted in military practice and serves as a conceptual foundation for contemporary strategies. The concept gained particular prominence following the publication of Frank Hoffman’s work *“Conflict in the 21st Century: The Rise of Hybrid Wars”* (2007), where hybrid threats are defined as a combination of conventional and unconventional instruments employed simultaneously to achieve political objectives.

Hybrid warfare functions as an instrument of state policy and is characterized by uncertainty, risk, and complexity. It integrates political, economic, and informational tools and can be applied across the spectrum from peacetime competition to open conflict. A key feature is the ability to achieve strategic objectives indirectly, minimizing the political risks associated with overt military confrontation.

In this context, the Russia–Ukraine war has become a key empirical case for analyzing the transformation of contemporary conflicts. The combination of military operations with cyber activities, information campaigns, economic pressure, and political coercion allows it to be considered a benchmark model of 21st-century hybrid warfare. This study focuses on the period 2014–2025 in order to synthesize key approaches to understanding this phenomenon.

Literature review

The academic literature offers various interpretations of hybrid warfare. F. Hoffman defines it as the simultaneous use of a tailored mix of conventional and irregular means, including terrorism and criminal activity. R. Glenn expands this definition by emphasizing the concurrent use of political, economic, social, and informational instruments, as well as the involvement of both state and non-state actors. P. Mansoor conceptualizes hybrid warfare as a conflict combining regular forces with irregular formations to achieve a shared political objective.

Scholars also highlight that hybrid warfare is grounded in non-linearity, ambiguity, and adaptability. It involves the simultaneous application of multiple tactics, which complicates its identification and counteraction. Consequently, related concepts such as “grey zone,” “non-linear warfare,” and “ambiguous warfare” are frequently used to capture the complexity of modern conflicts.

An important dimension is the duration of hybrid warfare and the capacity of actors to sustain prolonged confrontation. As noted by P. Mansoor, hybrid adversaries are capable of extending conflicts over time and space, testing the strategic endurance of their opponents. Public perception also plays a critical role, including the attitudes of populations in the conflict zone, the domestic audience, and the international community.

J. McCuen emphasizes that modern conflicts unfold simultaneously across multiple social arenas, while L. Freedman points to the challenges of coordinating regular and irregular forces within a unified strategy. At the same time, recent studies of the Russia–Ukraine war demonstrate the evolution of hybrid methods, including information suppression, logistical disruption, and economic pressure, as well as Ukraine’s adaptation through the integration of hybrid resistance elements into its defense strategy.

Materials and Methods

The study is based on a qualitative approach and aims to conceptualize the operational characteristics of hybrid warfare through an empirical analysis of the Russia–Ukraine conflict. The methodological framework combines comparative analysis, a systems approach, and synthesis of academic and applied sources, enabling a comprehensive examination of the multi-domain nature of contemporary conflicts.

The empirical basis of the study is formed through the analysis of a wide range of sources, including scholarly publications, analytical reports of international organizations, materials from

research centers, official government documents, and open-source intelligence (OSINT). Particular attention is given to publications in the field of security studies that address the nature of hybrid warfare, its instruments, and its evolution in the modern security environment. Sources were selected based on relevance, academic reliability, and timeliness, with a focus on the period 2014–2025, which covers the key stages of the Russia–Ukraine conflict.

The comparative analysis method was used to examine different theoretical approaches to defining hybrid warfare (in particular, the concepts of Hoffman, Glenn, and Mansoor) and their empirical manifestation in a specific conflict. This made it possible to identify similarities and differences between classical theoretical models and the practical implementation of hybrid strategies. The systems approach enabled the analysis of hybrid warfare as an integrated phenomenon encompassing political, informational, economic, cyber, and military components interacting within a unified operational environment.

The analytical procedure of the study included several stages. At the first stage, key characteristics of hybrid warfare were identified based on theoretical sources. At the second stage, these characteristics were empirically verified through the analysis of specific events and processes within the Russia–Ukraine war (cyber operations, information campaigns, economic pressure, the use of proxy forces, etc.). At the third stage, the results were synthesized to develop a coherent analytical model of hybrid warfare as a multi-domain phenomenon.

It is important to note that the study has certain limitations. In particular, the use of open sources may involve incomplete or potentially biased information. In addition, the dynamic nature of the ongoing conflict complicates the formulation of definitive conclusions, as many processes remain unresolved. Nevertheless, the applied methodology ensures a sufficient level of analytical validity and allows for well-grounded conclusions regarding the nature and evolution of hybrid warfare.

Thus, the combination of qualitative analysis, an interdisciplinary approach, and empirical verification ensures the scientific robustness of the findings and enables a deeper understanding of the complex structure of hybrid conflicts in the contemporary security environment.

Results

Hybrid Warfare in Ukraine: Operational Features and Defensive Countermeasures

In order to conceptualize the construct of hybrid warfare with greater analytical precision, it is necessary to highlight its distinguishing features. Although establishing a universally accepted framework remains challenging, the much-discussed hybrid war waged in Ukraine over the past decade has encompassed many, if not all of the commonly identified characteristics of this form of conflict. In this paragraph, we seek to delineate these features and substantiate them with empirical facts and relevant data.

1. Non-Military Asymmetric Warfare. The initial feature of the hybrid war in Ukraine is characterized by a concerted non-military asymmetric campaign designed to weaken Ukrainian resilience and influence both domestic and international perceptions without overtly crossing the threshold into full-scale conventional hostilities. It encompasses information, moral, psychological, ideological, diplomatic, and economic measures, which precede and shape the operational environment before kinetic conflict escalates (Iskandarov & Gawliczek, 2020a). Russia executed a large-scale cyber and information offensive immediately prior to and at the outset of the full-scale invasion. This phase can be traced back to 2014, following the occupation of Crimea. For instance, between 2014–2022 Russia launched over 1,200 cyberattacks against Ukrainian infrastructure (WiFiTalents, 2026). Cyber operations targeted energy sector, financial institutions, telecommunications and government services. The 2015–2016 power-grid cyberattack affected 230,000 electricity customers. Social-media propaganda generated billions of impressions globally (WiFiTalents, 2026). This feature was highly developed and long-lasting (2014–2022), however, the analysis will focus primarily on the immediate period surrounding the 2022 invasion and the

subsequent developments. Microsoft and cybersecurity analysts documented 15 Russian cyberattacks against Ukrainian targets in December 2021, rising to 125 attacks by March 2022, indicating a concerted escalation of cyber reconnaissance and penetration prior to the invasion. Preparatory operations focused on gaining access to critical infrastructure, government systems, and foreign-policy intelligence (Orenstein, 2022). On January 13–14, 2022, destructive malware known as WhisperGate struck Ukrainian government agencies, defacing around 70 official websites and corrupting data under the guise of ransomware (Mihaylov, 2025). On 14 January 2022 alone, more than a dozen Ukrainian government websites were disabled by hostile cyberattacks, including attacks on ministries and national security websites, underscoring the scale of pre-war cyber pressure. More than 3,000 DDoS attacks were recorded after 15 February 2022. Peak levels reached 275 attacks per day, with some exceeding 100 Gbps bandwidth (Ukrainska Pravda, 2022). HermeticWiper malware was deployed on 23 February 2022, only hours before Russian ground forces crossed Ukraine's borders and destroyed about 300 computer systems across government, financial, energy, and IT sectors (ESET, 2022). Both ESET and Microsoft observed that "the first shots were in fact fired in cyberspace," highlighting the operation as a coordinated and pre-planned cyber campaign (Smith, 2022; Mihaylov, 2025). Russian military intelligence (GRU) launched destructive data-wiping cyberattacks against hundreds of Ukrainian governmental, IT, energy, and financial systems. These destructive "wiper" operations were coordinated with the timing of imminent conventional military operations and intended to disrupt Ukrainian defensive coordination. Researchers observed increased Russian network reconnaissance in late 2021, involving attempts by state-linked groups such as the SVR-linked Nobelium to compromise Ukrainian communications, transportation, energy, defence, administrative, and diplomatic systems for intelligence purposes (Schulze and Kerttunen, 2023). On 24 February, the day the full-scale invasion began, IsaacWiper targeted at least one Ukrainian government network, further demonstrating the close synchronization between cyber operations and Russia's conventional military offensive (ESET, 2022). Large-scale propaganda campaigns and disinformation accompanied cyber operations. Empirical analysis of social media activity suggests that Russian-aligned propaganda reached significant audiences, with one corpus of approximately 349,000 pro-Russian messages garnering 251,000 retweets and an approximate reach of 14.4 million users in early 2022, amplified in part by automated bot networks (Geissler et al., 2022). Economic tools were weaponized to exert pressure on both Ukraine and Western societies. Western sanctions imposed on Russia, including exclusion from SWIFT and caps on oil prices were countered by Moscow's parallel import strategies and energy export diversification, enabling it to sustain wartime production despite punitive measures (Hirose, 2025). Bilateral trade between Russia and Ukraine plummeted by approximately 75% after 2014, contributing to economic contraction and loss of industrial capacity, a vulnerability exploited in subsequent hybrid campaigns (Zarembo and Solodkyy, 2021). Russia engaged in diplomatic efforts to create favorable narratives and fracture international support for Ukraine, including leveraging historical grievances, minority tensions within Ukraine, and geopolitical messaging to external audiences (Institute of Naval Forces of Ukraine, 2023). Ideological tactics sought to cultivate perceptions of Western fragmentation and to undermine Ukraine's legitimacy as a sovereign state, reinforcing narratives about Ukraine's alleged instability and the purported necessity of Russian intervention (Yakovenko and Piskorska, 2023).

Against the backdrop of non-military asymmetric warfare, Ukraine implemented rapid and effective cyber countermeasures. Most targeted websites were restored within hours, reflecting a highly responsive incident management system. Ukrainian CERT and security services actively detected and mitigated malware and phishing campaigns aimed at the energy, finance, and government sectors, preventing significant disruption and maintaining operational continuity (Lewis, 2022). As a result, although Russia achieved temporary disruption, it failed to precipitate a collapse of banking services, administrative paralysis, or a breakdown of national communications

prior to the invasion. This outcome can be assessed as an operational success for the defending party, namely Ukraine. Russia's cyber campaign did not neutralize Ukrainian state capacity before February 2022. Regarding information countermeasures, official communication campaigns warned citizens about cyber threats, while public statements attributing attacks to Russia were promptly released and false information was rapidly corrected. As a result, no large-scale panic occurred prior to the invasion, Ukrainian institutions continued to function normally, and both mobilization and government decision-making proceeded without interruption.

2. Special Operations Aimed at Misleading Political and Military Leaders. This feature of hybrid warfare involves coordinated special operations designed to mislead political and military leadership in the targeted state through a combination of intelligence, deceptive messaging, and psychological manipulation. These actions seek to distort decision-making, create false perceptions, and induce hesitation or miscalculation at critical moments (Iskandarov & Gawliczek, 2021). In the early months of Russia's 2022 invasion of Ukraine, false direct messages were sent to Ukrainian generals by actors posing as Russian commanders, urging surrender and promising safety. According to analysis by the British Royal United Services Institute, "almost all colonels and other senior officers" received such messages, aiming to undermine operational cohesion at the military leadership level. Fake accounts mimicking official Ukrainian military channels emerged immediately prior to and during the opening phases of the conflict. For instance, a fake Twitter account impersonating Ukraine's Armed Forces leadership was exposed in July 2022, illustrating how information manipulation directly targeted military command and control perceptions. Hybrid campaigns extended beyond immediate military messaging to broader influence operations that targeted political elites and international stakeholders with fabricated or misleading narratives. For example, Kremlin-linked disinformation networks disseminated claims of secret negotiations between Russia and Western governments about territorial concessions in exchange for political support, intended to sow confusion among Ukrainian policymakers and allies (Centre for Strategic Communications and Information Security, 2023). The Russian information ecosystem also employed sophisticated "doppelgänger" campaigns**,** which involved the creation of almost identical copies of Western news outlets and official pages to spread counterfeit stories. This campaign produced fake articles and statements designed to distort perceptions about Western political support and security commitments, thus complicating strategic decisions by both Kyiv and its partners (Langston, 2026). As part of hybrid deception, malicious actors have used AI-generated deepfake media portraying Ukrainian leaders making false statements, such as calls for surrender that risked influencing both internal and external perceptions of Ukraine's political unity and resolve. These synthetic media have been documented as part of coordinated misinformation operations intended to disrupt leadership communication (Petriv, 2024). Ukraine implemented a comprehensive set of countermeasures to mitigate hybrid operations aimed at misleading political and military leadership. These responses combined cyber defence, institutional coordination, rapid fact-checking, and proactive information operations, enabling authorities to preserve situational awareness and support informed decision-making. First, Ukraine significantly strengthened its cyber defence and incident response capabilities. The Computer Emergency Response Team of Ukraine (CERT-UA) registered 2,194 cyber incidents in 2022**,** including 1,148 critical high-level incidents**,** most of which were successfully mitigated before causing operational disruption. Cyberattacks occurred at an average rate of approximately 10 attacks per day**,** demonstrating the intensity of hybrid pressure on Ukrainian decision-making systems (Freedom House, 2023). Ukraine also established a structured institutional framework to counter information manipulation. The Center for Countering Disinformation, along with partner organizations, monitored hostile narratives and recorded a dramatic increase in disinformation campaigns, identifying 742 false messages in 2022 alone, compared to just 71 between 2019 and 2021. By 2023, this number had surpassed 1,450 identified disinformation narratives, highlighting the scope and intensity of Ukraine's monitoring

efforts (Burdiak, 2024). Ukraine also conducted coordinated public communication campaigns to counter deception efforts. Rapid official clarification of false claims, including fabricated surrender messages and deepfake videos helped prevent public panic and maintain confidence in national leadership. Although early deepfake videos and manipulated content reached millions of users online, their strategic impact was mitigated through prompt exposure and correction (Rehan, 2025). More broadly, Ukraine benefited from extensive international cooperation. Between December 2021 and December 2023, approximately 3,225 cyberattacks and cyber operations linked to the conflict were recorded and analyzed with the support of international partners. Concurrently, monitoring organizations identified around 470 websites actively disseminating pro-Kremlin disinformation, facilitating targeted countermeasures and the implementation of sanctions (Alliance for Peacebuilding, 2024). As a result of these combined efforts, Ukraine maintained the functionality of its command-and-control structures and curtailed the effectiveness of deception operations targeting political and military leaders. While hybrid operations remained persistent and adaptive, Ukraine's integrated cyber and information defenses substantially reduced the risk of strategic miscalculation or leadership paralysis during critical phases of the conflict.

3. Intimidation, Deception, and Bribery of Government and Military Officers. This feature of hybrid warfare encompasses coordinated efforts to intimidate, deceive, and co-opt government and military personnel, thereby undermining institutional integrity, encouraging dereliction of duty, or diverting resources away from effective defence. While outright coercion by adversary agents is difficult to quantify precisely, evidence from the Russia–Ukraine war reveals systemic corruption and intimidation that has affected officials' ability to perform their duties, both as a direct effect of hybrid pressures and as internal vulnerabilities exploited within the wider conflict environment. Patterns of corruption in mobilisation offices**,** combined with widespread public fatigue and socio-economic stressors caused by the ongoing war**,** have contributed to internal breakdowns of cohesion and trust in institutions, which are core targets of hybrid influence operations (Blakemore and Mankovska, 2025). Investigations revealed specific instances where officers accepted bribes of several thousand U.S. dollars to issue false medical or service-avoidance documents, with some transactions reported around $5,000 per individual and cases involving fictitious medical exemptions (Jankowicz, 2023). In another case, Ukrainian officials and employees within the defence sector were accused of embezzling nearly $40 million allocated for the procurement of artillery ammunition (Associated Press, 2024). A senior government figure was investigated for involvement in a $345,000 kickback scheme that resulted in significant losses to the state (The Guardian, 2025). Ukraine has implemented comprehensive institutional, legal, and operational countermeasures to address hybrid threats that exploit corruption, intimidation, and bribery within government and military structures. These measures have focused on both systemic vulnerabilities and specific incidents, helping to preserve institutional integrity and sustain effective national defense. In mid-2023, the President of Ukraine dismissed all 24 regional heads of military recruitment offices following accusations of bribery and intimidation connected to avoidance of military service. This action was taken in response to corruption scandals that implicated officials in taking cash and even cryptocurrency from those attempting to circumvent frontline deployment, and 112 criminal cases were opened against recruitment officials on these grounds (Kramer, 2023; Boffey, 2023; Eruygur, 2023). On 4 October 2024, Ukraine's security services detained Tetiana Krupa, head of the Medical-Social Expert Commission (MSEC) in Khmelnytskyi Oblast and a local Servant of the People deputy, after finding about $6 million in cash at her home. On 16 October 2024, journalist Yuri Butusov reported that 51 public prosecutors in the region had obtained disability certificates from the MSEK to claim pensions, including the regional prosecutor, who resigned. Similar abuses were found in other oblasts, with investigations showing 5–30% of prosecutors had falsified certificates. Several regional prosecutor heads resigned. In the aftermath of these scandals, Ukraine's parliament enacted legal reforms to digitize and modernize MSEC

procedures, aiming to prevent similar abuses in the future (Jędrysiak, 2024). On 22 October 2024, the Security Service of Ukraine (SBU) revealed eight organised crime rings linked to MSEK members, annulled 4,106 fraudulent disability certificates, and began reviewing 2,400 more. The SBU exposed six mobilization evasion schemes across multiple regions, involving fake medical certificates and illegal transport for draft dodgers; 19 organisers were detained (LB.ua, 2025). President Volodymyr Zelensky ordered audits of MSEK members' assets and disability pensions (Jędrysiak, 2024). In August 2025, Ukraine's National Anti-Corruption Bureau (NABU) and the Specialized Anti-Corruption Prosecutor's Office (SAPO) uncovered a major bribery and kickback scheme involving a member of parliament, local officials, and National Guard personnel linked to inflated military procurement contracts for drones and electronic warfare equipment. Kickbacks reportedly reached up to 30% of contract values. For example, a contract worth approximately UAH 10 million (about US$239,000) generated roughly US$80,000 in illicit gains for the individuals involved. As a result, four suspects were detained and removed from their posts, while government authorities publicly reaffirmed a zero-tolerance policy toward wartime corruption that could undermine defence capabilities (Tyshchenko, 2025). These sources document concrete institutional countermeasures, including actions by the SBU, NABU, and SAPO, as well as legal reforms such as the digitization of disability adjudication procedures and strengthened personnel accountability through dismissals and prosecutions. Together, these measures reduced opportunities for hybrid threats to exploit internal corruption and influence critical decision-making processes.

4. Propaganda to Increase Public Discontent and Escalate Subversion. In this feature of hybrid warfare, propaganda becomes a central tool to intensify societal discontent, undermine trust in government, and escalate subversion within the targeted population. This phase relies on sustained information operations across media platforms, automated bot networks, and fabricated narratives that blur fact and fiction, with the objective of weakening social cohesion and reducing public support for the state's defence efforts (Iskandarov, & Gawliczek, 2020d). Russia's hybrid strategy has deployed large-scale automated propaganda across social media to influence public sentiment in occupied and contested regions. Between January 2024 and April 2025, at least 3,634 pro-Kremlin bot accounts posted more than 316,000 messages targeting civilians in regions such as Zaporizhzhia, Donetsk, and Kherson, seeking to weaken Ukrainian identity and legitimize Russian control by spreading tailored narratives that blame Ukraine for local hardships (e.g., blackouts, economic woes) (Riley-Smith, 2025). Analyses of social media activity during the invasion have shown that approximately 349,000 pro-Russian messages received roughly 251,000 retweets and reached around 14.4 million users, demonstrating the extensive reach of propaganda and its potential impact on public attitudes (Geissler et al., 2022). Disinformation narratives have also focused on exaggerating Ukrainian casualties, portraying Western sanctions as harmful to local economies, and disputing the credibility of Ukraine's leadership, all designed to sow doubt and social frustration both within Ukraine and among its supporters in Europe (Bryjka, 2024). The scale of propaganda efforts reflects their prioritization within hybrid warfare strategy: Russia allocated approximately $1.4 billion for propaganda in its 2025 budget, underlining the role of information operations in eroding societal resilience and encouraging acceptance of "peace at any cost" narratives (Centre for Strategic Communications and Information Security, 2025). Ukraine has implemented a comprehensive set of countermeasures to neutralize propaganda intended to fuel public discontent and intensify subversive activity. These measures combine institutional coordination, technological monitoring, strategic public communication, and international cooperation. The Center for Countering Disinformation (CCD), operating under the National Security and Defense Council, coordinates national responses to propaganda and information manipulation while monitoring threats across political, military, and societal domains (Center for Countering Disinformation, 2023). Since its establishment, the CCD has identified 21,335 information threats, demonstrating the scale and intensity of its monitoring activities. The Center's materials have

generated an estimated 1.7 billion cumulative media impressions, contributing to the dissemination of verified information and the countering of hostile narratives. The CCD cooperates with 65 institutions and partners across 30 countries, including NATO-related bodies, reflecting the multinational character of these counter-disinformation efforts (National Security and Defense Council of Ukraine, 2025). The Security Service of Ukraine (SBU) shut down 21 bot farms operating over 150,000 fake accounts, significantly curbing the spread of destructive online narratives. Authorities also dismantled 15 coordinated disinformation networks and banned 137 foreign propagandists engaged in online influence operations (Freedom House, 2022). The Centre for Strategic Communications introduced the "Spravdi Bot" reporting system, which processed around 1,000 disinformation alerts in its first month, enabling rapid fact-checking and prompt correction (Spravdi, 2023). The CCD identified 365 hostile Telegram channels, 65 hostile X accounts, and 83 hostile TikTok channels, many of which were subsequently blocked. In cooperation with platform administrators, more than 200 hostile YouTube channels and 24 TikTok channels were removed. Ukrainian monitoring teams track hundreds of information sources daily, including 449 Telegram channels and 200 X accounts, allowing near real-time detection of hostile narratives (Center for Countering Disinformation, 2025). Authorities exposed fake intelligence chatbots designed to harvest personal data and mislead civilians, demonstrating proactive detection of subversive digital tools (Detector Media, 2024). Ukraine invested in strengthening societal resilience against propaganda. In 2022, the Centre for Strategic Communications organized over 30 training programs for more than 700 civil servants, military personnel, and educators, focusing on detecting and countering disinformation. In 2023, additional efforts included 102 training events attended by 837 participants, encompassing government officials and military personnel (Spravdi, 2023). Despite large-scale propaganda campaigns, including networks of 3,634 pro-Kremlin bots producing over 316,000 messages in occupied regions Ukraine's integrated countermeasures effectively limited attempts to generate widespread social unrest (Dukach, et al., 2025). Overall, Ukraine's response illustrates a multi-layered counter-propaganda strategy that combines institutional coordination, technological monitoring, bot-network disruption, rapid fact-checking, public education, and international cooperation. These measures helped preserve social cohesion and public confidence in national defense, diminishing the effectiveness of propaganda-driven subversion during the conflict.

5. Imposition of No-Fly Zones, Blockades, and the Extensive Use of Private Military Companies in Concert with Armed Opposition Units. This feature of hybrid warfare is marked by the transition from predominantly covert and informational measures to overt coercive instruments, including the imposition of de facto no-fly zones, maritime blockades, and the systematic employment of private military companies (PMCs) operating alongside proxy or separatist armed formations (Iskandarov & Gawliczek, 2025). In the Ukrainian case, several empirically verifiable developments illustrate this feature. Following the occupation and subsequent annexation of Crimea in March 2014, Russia rapidly established effective control over Crimean airspace, integrating it into its Southern Military District air defence architecture. The deployment of advanced S-400 Triumf surface-to-air missile systems (range up to 400 km) in Crimea significantly expanded Russia's anti-access/area-denial (A2/AD) envelope over the Black Sea region, effectively creating a de facto no-fly zone over parts of southern Ukraine and adjacent maritime air corridors (BlackSeaNews, 2024). After the full-scale invasion in February 2022, Ukraine closed its civilian airspace entirely, by contrast, Russia sought to deny Ukraine effective use of its own airspace through long-range air defence systems and missile strikes on airbases, destroying or damaging multiple Ukrainian airfields in the opening days of the invasion (Vakulina, 2025). After withdrawing from the 2022 Black Sea Grain Initiative, Russian authorities threatened maritime approaches to Ukrainian ports and effectively hindered commercial access**,** including declaring that ships entering Ukrainian ports might be treated as potential military supply carriers. This has had significant implications for Ukraine's export economy and global food markets (IntSecurity.org, 2023). Russia's

efforts to control sea lanes and apply pressure on cities such as Odessa through sustained missile and drone strikes on port infrastructure are widely reported as attempts to isolate Ukraine economically and restrict its maritime trade (Dysa, 2025). Ukraine was heavily dependent on maritime trade prior to the full-scale invasion (with around 60 % of total trade conducted by sea**),** and Russia's actions in blocking sea access have drastically shifted trade patterns and imposed economic strain (Romaniuk, 2024). Wagner Group has been extensively involved in hybrid and conventional phases of the Russia–Ukraine war: it operated in Crimea in 2014 during the annexation, participated with separatist forces in Donbas, and later deployed significant numbers of fighters (estimated in the tens of thousands by U.S. and independent sources) in Ukraine's frontline operations. In late 2022 and 2023, Wagner forces were heavily engaged in battles, such as Bakhmut and redeployed throughout Donetsk and other occupied regions, illustrating their use as a proxy combat force alongside regular Russian troops (Bryjka, 2023; Górka, 2023). Ukraine has been unable to secure a Western-backed no-fly zone due to allied reluctance to engage directly with Russia, which possesses the world's largest air defense systems, such as the S-400, and would likely view such a move as an escalation. NATO has consistently rejected calls for a no-fly zone, citing concerns over direct confrontation with Russian aircraft. Former NATO officials have explained that enforcing such a zone would require strikes against Russian air defenses, thereby risking a broader conflict (Eruygur, 2025). Ukraine is exploring joint ventures with Western allies to bolster its ballistic and air-defense capabilities, particularly in light of ammunition shortages for Patriot missile systems (Hunder, 2026). These measures aim to mitigate Russian air superiority over critical infrastructure, even though full enforcement of a no-fly zone remains politically and militarily unattainable. Ukrainian leadership and government officials have publicly called for the Wagner PMC to be recognized internationally as a terrorist organization, seeking to delegitimize and undermine their combat operations and logistical support. Ukrainian forces have actively engaged and weakened PMC formations on the battlefield: for example, Russian units affiliated with Wagner were reportedly replaced by regular Russian troops in key sectors as Ukrainian resistance and attrition reduced the effectiveness of PMC deployments in 2023. Ukraine has also conducted deep-strike operations against Russian infrastructure, targeting airfields and fuel pipelines deep within territory controlled by Moscow, thereby undermining the logistical bases that sustain both Russian regular forces and PMC units (Ilyushina, 2025).

6. Commencement of Military Action Preceded by Large-Scale Intelligence and Reconnaissance Operations. This feature of hybrid warfare marks the transition from preparatory and covert actions into full-scale military operations. Crucially, this kinetic phase is preceded by extensive and multi-domain reconnaissance, subversive missions, and intelligence collection**,** including activities in space, radio/signal intelligence (SIGINT), electronic warfare, diplomatic spheres, cyber domains, and industrial espionage (Iskandarov et al., 2024). These intelligence measures are designed to shape the battlefield, undermine adversary decision-making, and maximise the effectiveness of subsequent offensive action. Russian intelligence groups from the Federal Security Service (FSB) and other services were linked to cyberattacks and intelligence operations targeting Ukrainian state and military infrastructure well before the kinetic invasion began (Schulze and Kerttunen, 2023). Hundreds of cyberattacks targeted Ukrainian infrastructure, frequently synchronized with conventional military operations, thereby signalling a systematic effort at intelligence preparation of the battlefield (Knutson, 2022). Russia extensively employed unmanned aerial vehicles (UAVs) to conduct reconnaissance, support artillery targeting, and enhance real-time battlefield awareness, thereby constituting a critical component of its intelligence, surveillance, and reconnaissance (ISR) architecture. ISR systems facilitated artillery strikes and precision targeting, albeit at times with operational delays attributable to technical limitations (Bernat, 2024). European counterintelligence cooperation in the first years of the war led to the arrest of hundreds of individuals involved in espionage or sabotage on behalf of Russian

intelligence, many of whom had conducted operations prior to and during the early stages of the invasion (Riehle, 2024). Ukrainian military intelligence established units such as the Black Winter Group**,** a spetsnaz reconnaissance and sabotage unit active in early battles in 2022, demonstrating how reconnaissance forces on both sides played a role throughout initial combat phases. Similarly, units like the Kraken Regiment**,** formed for reconnaissance and sabotage actions, operated concurrently with overt combat in early campaigns (Harward et al., 2025). Prior to 24 February 2022, Russia amassed between 150,000 and 190,000 troops and approximately 120 Battalion Tactical Groups (BTGs) along Ukraine's borders, in Belarus, and in annexed Crimea, demonstrating preparation for offensive operations (Bowen, 2023). Western intelligence, particularly that of the U.S. disclosed Russia's operational plans and anticipated invasion timeline prior to the onset of hostilities, thereby evidencing a profound penetration into Russian military decision-making and intent (Takagi, 2023). Ukraine's countermeasures during the initial phase of the 2022 invasion were multi-layered, integrating cyber defence, intelligence reform, territorial mobilisation, and international coordination. Ukraine rapidly migrated key government data and services to commercial cloud providers such as Amazon Web Services (AWS) and other platforms to safeguard them from Russian cyber and kinetic attacks. As a result, missile strikes or the seizure of local servers did not compromise or destroy critical state data **(**Bassett, 2025). Ukraine's cyber agencies, including CERT-UA, sustained operations during the initial wave of Russian cyberattacks in January–February 2022, including the deployment of the HermeticWiper and AcidRain malware. Support from Western cybersecurity firms and intelligence partners enhanced detection capabilities and helped block malicious traffic (Chochtoulas, 2023). Ukraine formalised its Territorial Defence Forces (TDF) as a separate branch on 1 January 2022 in response to Russia's military build-up. On 11 February 2022, the planned volunteer reserve pool was expanded from 1.5 million to 2 million. Within days of the invasion, over 110,000 volunteers had joined the Territorial Defence Forces, taking up positions alongside regular forces to defend cities including Kyiv, Kharkiv, Chernihiv, and Zaporizhzhia (Ministry of Defence of Ukraine**,** no date). Ukrainian forces leveraged AI and automated tools to rapidly process ISR data from platforms such as UAS drones, shortening detection-to-action timelines and improving responses to Russian reconnaissance efforts (Pusztaszeri & Harding, 2025). Ukraine received early warnings from Western intelligence partners in late 2021 and early 2022 regarding Russian troop buildups and cyber threats, helping to mitigate strategic surprise. Public reporting indicates that Russia conducted extensive cyber probing and deployed destructive malware in the period immediately preceding the invasion. Migration to cloud services, combined with resilient communications, including Starlink as a fallback during the early months of the war enabled Ukraine to maintain government and military communications despite Russian cyber and kinetic pressures (Chochtoulas, 2023). Although Russia employed both kinetic and cyber tactics from early 2022, Ukraine avoided widespread service failures, such as mass power grid collapses or the loss of government networks, demonstrating the effectiveness of its cyber resilience and mobilised defence posture **(**Bassett, 2025). Ukraine's multi-layered countermeasures integrated cyber resilience, volunteer mobilisation, international cooperation, intelligence sharing, and advanced information systems to counter Russia's multi-domain offensive. These efforts helped stabilise national defence structures, ensure continuity of government, and thwart Russia's early objectives of rapid collapse and decapitation.

7. Targeted Information, Electronic Warfare, Aerospace Operations, and High-Precision Strikes. This feature represents a full-spectrum escalation in hybrid warfare, where preparatory intelligence, reconnaissance, and subversive operations converge with direct kinetic and multi-domain attacks. This phase is marked by: Continuous information operations and psychological warfare targeting command structures and civilian populations; Electronic warfare (EW) campaigns disrupting communication, navigation, and radar systems; Aerospace operations**,** including repeated air-force harassment and missile strikes; High-precision weapons employment launched

from land, sea, air, and unmanned platforms. This multi-domain integration aims to maximize operational impact, degrade enemy combat effectiveness, and create persistent uncertainty for both military and civilian decision-makers. Russian forces have consistently deployed psychological operations to amplify fear, confusion, and misinformation**,** such as broadcasting false surrender orders or exaggerating battlefield losses. Example: In early 2023, Russian disinformation campaigns claimed that Ukrainian forces had collapsed in Kharkiv, coinciding with limited but coordinated artillery and missile strikes. Analysts noted these campaigns were intended to influence Ukrainian morale and disrupt operational planning**.** Russian forces have consistently deployed psychological operations to amplify fear, confusion, and misinformation**,** such as broadcasting false surrender orders or exaggerating battlefield losses (Reuters, 2023). EW has been used extensively to jam communications, GPS signals, and radar systems**,** degrading the Ukrainian Armed Forces' command, control, and situational awareness. According to NATO reports, over 1,200 instances of electronic warfare jamming and interference were documented between February 2022 and mid-2023**,** including the use of mobile EW systems and air-based jamming units targeting drones, artillery, and tactical radios (Le Gargasson and Black, 2025). EW operations were synchronized with UAV and artillery strikes, demonstrating multi-domain coordination that is characteristic of hybrid warfare in this phase. Russian air forces and tactical aviation continuously conducted harassment raids, reconnaissance flights, and missile attacks targeting Ukrainian supply lines, airfields, and command centers. For example, between March and June 2022, Ukrainian air-defense systems intercepted over 500 cruise and ballistic missiles, indicating the scale and intensity of aerospace operations (Welsch, 2026). Persistent air activity contributed to psychological pressure, limited freedom of movement, and disrupted logistics. Investigators from the Eyes on Russia project, using open-source verification methods, have recorded and verified 2,642 incidents involving attacks on hospitals, schools, churches, and energy supply infrastructure in Ukraine since the Russian full-scale invasion began in February 2022**.** These figures encompass missiles, drones, and other force applications that resulted in infrastructure damage (Centre for Information Resilience, 2024). Platforms included ships in the Black Sea, strategic bombers, fighter aircraft, and mobile missile launchers, illustrating cross-domain strike coordination**.** In response to Russia's multi-domain escalation, Ukraine implemented a comprehensive array of countermeasures designed to mitigate Russia's hybrid warfare operations across multiple domains. These responses integrated air defence modernisation, electronic warfare (EW) capabilities, counter-information measures, and critical infrastructure protection, thereby demonstrating a high degree of adaptive resilience against coordinated kinetic and non-kinetic attacks. Ukraine invested heavily in electronic warfare and counter-unmanned aerial system (C-UAS) capabilities to reduce the effectiveness of Russian drones and precision-guided strikes. Electronic warfare systems proved capable of neutralising a substantial proportion of Russian UAV attacks. By mid-2025, Ukrainian jamming systems were reportedly responsible for the failure of up to 60% of Russian drones, demonstrating the growing effectiveness of EW as a critical defensive instrument (Welsch, 2025). Ukraine also deployed mobile interception units and acoustic early-warning systems that significantly improved detection and response times against UAV attacks. These measures enabled interception rates of approximately 85–90% for cruise missiles and around 80–87% for drones, depending on operational conditions and the intensity of attacks. Ukraine further conducted deep strikes against Russian drone production facilities, reducing the number of long-range drones deployed after August 2025 and demonstrating the development of offensive counter-EW and counter-industrial capabilities (Butterworth-Hayes, 2026). Layered air defence systems constituted the core of Ukraine's response to Russian aerospace operations and high-precision strikes. Ukrainian air defence forces intercepted a substantial proportion of incoming threats. Cruise missile interception rates frequently reached 65–90%, while ballistic missile interception averaged approximately 25%, reflecting the technical complexity and operational difficulty of engaging high-speed ballistic targets. Air-based interception capabilities also expanded

significantly. Since mid-2024, Ukrainian fighter aircraft have intercepted more than 1,300 aerial threats, thereby enhancing the effectiveness of Ukraine's integrated air defence system and contributing to a more layered and flexible defensive architecture (Welsch, 2025). During large-scale Russian attacks, Ukrainian air defences demonstrated substantial operational effectiveness. In one major aerial assault in 2026, Ukraine reportedly shot down 374 drones and 32 missiles out of 420 drones and 39 missiles launched, illustrating the resilience and sustained operational capacity of Ukraine's air defence network despite continuous pressure (Reuters, 2026). Ukraine pioneered the operational use of interceptor drones as a cost-effective air defence solution. By early 2026, interceptor UAVs were responsible for destroying approximately 30 % of Russian aerial threats, demonstrating the growing importance of unmanned systems within modern air defence architectures (Loh, 2026). Ukraine also expanded passive defensive measures. Plans were implemented to install anti-drone protective systems along approximately 4,000 km of frontline roads, aimed at safeguarding logistics routes and reducing operational vulnerability to drone strikes (Reuters, 2026). Ukraine implemented extensive civil defence and infrastructure protection measures to mitigate the strategic impact of Russian precision strikes. These measures included hardened energy facilities, dispersed logistics networks, and rapid repair capabilities. Despite approximately 56,700 aerial attacks in 2025, the majority were either intercepted or otherwise mitigated, enabling critical infrastructure to maintain operational continuity (Welsch, 2025). Civil defence measures and early-warning systems significantly reduced casualties and bolstered societal resilience, thereby diminishing the psychological impact and intended coercive effect of Russian strike campaigns.

With the aforementioned features, we have sought to encapsulate the principal dynamics observed in the Russia–Ukraine war. However, within the framework of hybrid warfare, belligerents systematically exploit every available opportunity, irrespective of scale or intensity to erode the adversary's resilience. In this regard, the ongoing conflict in the Middle East, particularly a potential confrontation between the U.S. and Iran, exerts a significant, albeit indirect impact on the Russia–Ukraine war. Analysts broadly concur that such developments tend to advantage Russia while disadvantaging Ukraine, notwithstanding certain nuanced or mixed effects. This dynamic operates through several interrelated mechanisms. First, global attention is inevitably diverted. The emergence of a new conflict in the Middle East generates a form of "information overload" within the international system. Under these conditions, Russia can strategically amplify narratives such as "the West perpetuates instability globally" or "Ukraine is no longer a strategic priority." The proliferation of competing crises dilutes the consistency and salience of Ukraine's messaging. Diplomatic engagement, and political bandwidth are similarly redirected toward the Middle Eastern crisis. Western leaders are compelled to devote substantial time and resources to crisis management in that region, thereby reducing both the intensity of diplomatic efforts related to Ukraine and the overall level of political pressure exerted on Russia. Consequently, Ukraine experiences a decline in international visibility, whereas Russia gains greater latitude to shape global perceptions. This constitutes a quintessential manifestation of information warfare, in which distraction functions as a highly effective instrument. Second, military assistance to Ukraine risks being reallocated against the backdrop of finite Western stockpiles. High-demand systems, such as Patriot air defense platforms are simultaneously required in multiple theatres: in Ukraine, to counter Russian missile strikes, and in the Middle East, to defend against Iranian missile and drone threats. This competition for limited resources may constrain the volume, timeliness, and sustainability of support provided to Ukraine. Beyond these factors, the U.S. and its allies are compelled to reallocate strategic assets toward the Middle East, thereby affording Russia greater operational latitude in both Ukraine and the broader European theatre. As the Middle East assumes heightened strategic priority, Ukraine is likely to face reduced access to military assistance, accompanied by delays in delivery schedules. While the West retains the aggregate capacity to

sustain engagement in two major conflicts simultaneously, it is unlikely to do so with equal intensity or resource commitment. Consequently, Ukraine risks being relegated to a secondary strategic priority. Third, hybrid warfare intrinsically leverages economic instruments as tools of coercion. A conflict involving Iran has already exerted upward pressure on global oil prices, driven by disruptions in critical transit chokepoints such as the Strait of Hormuz. Given that Russia remains a major oil exporter, elevated energy prices directly enhance its fiscal capacity. This dynamic, in turn, dilutes the effectiveness of Western sanctions by increasing Russian state revenues, thereby enabling Moscow to sustain and potentially intensify its war effort in Ukraine. The principal countervailing factor lies in the disruption of Russia's cooperation with Iran, which has been a significant supplier of unmanned aerial systems. However, this constraint appears to be of diminishing importance. Russia has increasingly localized production and adapted its defense-industrial base to compensate for external dependencies. Consequently, the loss of Iranian support is likely outweighed by the financial gains derived from elevated energy prices and the strategic advantages conferred by Western distraction. In sum, Russia stands to benefit from systemic instability that strains Western cohesion and resources, while Ukraine is compelled to continuously recalibrate its strategy to maintain international relevance. Simultaneously, the Middle East emerges as an additional arena of indirect geopolitical competition, further complicating the strategic environment.

Discussion

The findings confirm that hybrid warfare extends beyond the traditional understanding of a combination of irregular or non-kinetic actions and increasingly represents a comprehensive multi-domain strategy. In this context, the Russia–Ukraine war demonstrates not only the application of hybrid instruments but also their evolution toward the integrated use of political, informational, economic, cyber, and military tools within a unified operational design.

A comparison of the results with classical concepts of hybrid warfare (Hoffman, Mansoor, Glenn) indicates their partial relevance, while also revealing their limitations. In particular, traditional definitions emphasize the combination of regular and irregular forces but insufficiently account for the role of digital technologies, cyberspace, and the information environment as independent operational domains. This study shows that these components play a decisive role in the early stages of conflict, shaping the conditions for subsequent military escalation.

An important theoretical implication is the conceptualization of hybrid warfare as a continuum integrating non-kinetic and kinetic forms of influence. This approach helps overcome the dichotomy between "hybrid" and "conventional" warfare often present in the literature. Empirical evidence suggests that these forms are not mutually exclusive but operate in a complementary manner. At the same time, it is important to critically note that an overly broad interpretation of the concept of hybrid warfare may lead to analytical ambiguity, where virtually any contemporary conflict could be classified under this term.

Particular attention should be given to the role of state resilience as a key determinant in countering hybrid threats. The Ukrainian case demonstrates that even under conditions of intense external pressure, a state can maintain institutional functionality, ensure continuity of governance, and preserve public trust. This has been largely achieved through a combination of cyber defense, strategic communication, anti-corruption measures, and international support. These findings align with approaches that consider resilience a central element of modern security.

At the same time, the analysis reveals several problematic aspects. First, the issue of measuring the effectiveness of hybrid operations remains unresolved, as their outcomes are often indirect and delayed. Second, the difficulty of distinguishing targeted information influence from general informational noise complicates the assessment of its actual impact on society and decision-making processes. Third, there is a risk of overestimating the role of external actors while underestimating internal structural weaknesses that may act as catalysts for hybrid threats.

From a practical perspective, the results highlight the need to shift from reactive to proactive strategies in countering hybrid warfare. This includes the development of integrated early-warning systems, strengthening interagency coordination, investing in cybersecurity, and enhancing public media literacy. At the same time, effective countermeasures are not possible without international cooperation, as demonstrated by the Ukrainian experience.

Thus, the findings not only refine the theoretical foundations of hybrid warfare but also indicate the need for further development of methodological approaches to its analysis, particularly through the integration of qualitative and quantitative methods for assessing complex multi-domain processes.

Conclusion

The scholarly body of work on the Russia–Ukraine War illustrates how hybrid warfare has transcended theoretical debate to become a practical framework for analyzing modern conflict. While there remain definitional and conceptual challenges, the conflict serves as an indispensable case study for military strategists, policymakers, and academics exploring the contours of hybrid warfare. This study examined the operational characteristics of hybrid warfare through the empirical case of the Russia–Ukraine war. By analysing multiple dimensions of the conflict, including cyber operations, information warfare, intelligence activities, economic pressure, proxy forces, and conventional military operations—the paper sought to clarify how hybrid strategies function in practice and how states can respond effectively to such multidimensional threats. The analysis demonstrates that hybrid warfare should be understood as a coordinated and multi-domain strategy integrating both non-military and military instruments. Russia's approach in Ukraine illustrates how cyberattacks, disinformation campaigns, diplomatic pressure, economic measures, and intelligence operations were employed in the preparatory stages of conflict in order to shape the operational environment before the escalation of large-scale military hostilities in 2022. These non-kinetic measures were designed to weaken Ukrainian resilience, influence public perceptions, and create favourable conditions for subsequent military operations. At the same time, the findings indicate that hybrid warfare evolves progressively from covert and indirect activities toward overt military confrontation. The conflict demonstrates how information operations, electronic warfare, aerospace attacks, and high-precision strikes can be integrated into a unified operational framework alongside conventional forces. The Russia–Ukraine war therefore illustrates the transformation of hybrid warfare into a continuum of multi-domain conflict, where the boundaries between political, informational, cyber, and military instruments become increasingly blurred. A central conclusion of this study is that the effectiveness of hybrid strategies depends not only on the capabilities of the attacking state but also on the resilience of the targeted society and its institutions. Ukraine's experience shows that coordinated countermeasures—including cyber defence, strategic communication, institutional reforms, international cooperation, and military adaptation—can significantly reduce the effectiveness of hybrid operations. Despite extensive cyberattacks, propaganda campaigns, and economic pressure, Ukrainian institutions maintained operational continuity, while public cohesion and international support remained largely intact. Furthermore, the case highlights the growing importance of technological integration in contemporary warfare. Cyber capabilities, electronic warfare systems, unmanned aerial vehicles, and precision-guided weapons played a central role in shaping the operational environment of the conflict. These developments suggest that hybrid warfare increasingly relies on the interaction between digital and kinetic domains, requiring states to develop integrated defence architectures capable of responding to complex multi-domain threats. In conclusion, the Russia–Ukraine war provides one of the most comprehensive contemporary examples of hybrid warfare in practice. The conflict demonstrates how modern warfare combines political, informational, economic, cyber, and military instruments within a single strategic framework. At the same time, the Ukrainian response illustrates that

effective resilience, supported by institutional coordination, technological adaptation, and international partnerships can substantially limit the strategic impact of hybrid aggression. These insights contribute to a deeper understanding of hybrid warfare and provide valuable lessons for states seeking to strengthen their capacity to deter and counter multidimensional security threats in the evolving landscape of international conflict.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Associated Press. (2024). *Ukraine says corrupt officials stole $40 million meant to buy arms for the war with Russia*. https://apnews.com/article/ukraine-russia-war-corruption-476d673cc64a4b005c7ee8ed5f5d5361

Alliance for Peacebuilding. (2024). *Ukraine call to action: Combat mis/disinformation and promote cybersecurity in Ukraine and globally*. https://www.allianceforpeacebuilding.org/ukraine-call-to-action-combat-misdisinformation-and-promote-cybersecurity-in-ukraine-and-globally

Atlamazoglou, S. (2024, October 31). Russia's elite Spetsnaz special forces "devastated" in Ukraine war. *The National Interest*. https://nationalinterest.org/blog/buzz/russias-elite-spetsnaz-special-forces-devastated-ukraine-war-213488

Bassett, L. (2025). Silicon shadow: The influence of big tech in Russo-Ukrainian cyber warfare. *Cambridge Journal of Political Affairs, 5*(1), 70–116. https://www.cambridgepoliticalaffairs.co.uk/2025/01/14/silicon-shadow/

Bernat, P. (2024). *The evolution of Russian ISR satellite capabilities following the full-scale aggression on Ukraine (2022–2024)* [Conference presentation]. https://www.researchgate.net/publication/386177279

Blakemore, C., & Mankovska, O. (2025). Internal corruption as a mechanism of hybrid occupation: Strategic dimensions of state capture. *ResearchGate*. https://www.researchgate.net/publication/400556966

BlackSeaNews. (2024, October 16). *Review and database of Ukrainian attacks on the occupied Crimea, Russian ships and facilities on the Black Sea coast*. https://www.blackseanews.net/en/read/223691

Boffey, D. (2023, August 11). Zelenskiy sacks military recruitment heads over frontline bribes scandal. *The Guardian*. https://www.theguardian.com/world/2023/aug/11/zelenskiy-sacks-all-military-recruitment-heads-over-frontline-bribes-scandal-ukraine

Bowen, A. S. (2023). *Russia's war in Ukraine: Military and intelligence aspects* (CRS Report R47068). Congressional Research Service. https://www.congress.gov/crs-product/R47068

Bryjka, F. (2024). *Russia intensifies disinformation offensive against Ukraine* (PISM Bulletin No. 46). Polski Instytut Spraw Międzynarodowych. https://www.pism.pl/publications/russia-intensifies-disinformation-offensive-against-ukraine

Bryjka, F. (2023). *Wagner group transforms in the wake of the war in Ukraine*. Polski Instytut Spraw Międzynarodowych. https://pism.pl/publications/wagner-group-transforms-in-the-wake-of-the-war-in-ukraine

Burdiak, P. (2024). *A malicious alliance: How cyberattacks and disinformation are synchronously destabilizing the digital space of Ukraine*. Centre for Democracy and Rule of Law (CEDEM). https://cedem.org.ua/wp-content/uploads/2024/12/CEDEM_cyberdis_eng.pdf

Butterworth-Hayes, P. (2026, February 2). Ukraine's counter-UAS interception rate fell from 84% in November to 81% in December. *Unmanned Airspace*. https://www.unmannedairspace.info/counter-uas-systems-and-policies/ukraines-counter-uas-interception-rate-fell-from-84-in-november-to-81-in-december/

Center for Countering Disinformation. (2023). *About the Center for Countering Disinformation*. https://cpd.gov.ua/en/docs/about-center-for-countering-disinformartion/

Center for Countering Disinformation. (2025). *The Center held a press conference on the results of its work*. https://cpd.gov.ua/en/events-en/the-center-held-a-press-conference-on-the-results-of-its-work/

Centre for Information Resilience. (2024, November 23). *Open source investigators verify over 2,600 attacks on Ukraine's hospitals, schools, churches and energy supply since Russian invasion*. https://www.info-res.org/eyes-on-russia/articles/open-source-investigators-verify-over-2600-attacks-on-ukraines-hospitals-schools-churches-and-energy-supply-since-russian-invasion/

Centre for Strategic Communications and Information Security. (2023). *How Russian special services mislead relatives of Ukrainian military*. https://spravdi.org/en/how-russian-special-services-mislead-relatives-of-ukrainian-military/

Centre for Strategic Communications and Information Security. (2025, February 24). *Poisonous narratives: How Russia's information warfare strategy against Ukraine has evolved*. Ukrinform. https://www.ukrinform.net/rubric-ato/3965985-poisonous-narratives-how-russias-information-war

Chochtoulas, A. (2023). *Insights from the Ukrainian cyber battlefield: Is the private sector a game changer?* Joint Air Power Competence Centre. https://www.japcc.org/articles/insights-from-the-ukrainian-cyber-battlefield/

Detector Media. (2024). *DisinfoChronicle: Kremlin disinformation daily chronicle – 19 September 2024*. https://disinfo.detector.media/en/day/19-09-2024

Dukach, Y., Adam, I., & Furbish, M. (2025). *Digital occupation: Pro-Russian bot networks target Ukraine's occupied territories on Telegram*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report-russian-bot-networks-occupied-ukraine/

Dysa, Y. (2025, December 20). Escalating Russian airstrikes aim to cut Ukraine off from sea. *Reuters*. https://www.reuters.com/world/europe/russia-hits-ports-bridge-escalating-strikes-ukraines-odesa-region-2025-12-20/

Eruygur, B. (2025). Medvedev says no-fly zone over Ukraine will mean NATO-Russia war. *Anadolu Agency*. https://www.aa.com.tr

Eruygur, B. (2023, August 17). Ukrainian president adopts decree dismissing regional military conscription officials. *Anadolu Agency*. https://www.aa.com.tr

ESET. (2022). *IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine*. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

Eurasia. (2024, October 17). *Assessing Russian military adaptation in 2023*. https://eurasia.ro/2024/10/17/assessing-russian-military-adaptation-in-2023/

Freedom House. (2022). *Ukraine: Freedom on the Net 2022*. https://freedomhouse.org/country/ukraine/freedom-net/2022

Freedom House. (2023). *Ukraine: Freedom on the Net 2023*. https://freedomhouse.org/country/ukraine/freedom-net/2023

Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2022). Russian propaganda on social media during the 2022 invasion of Ukraine. *arXiv*. https://arxiv.org/abs/2211.04154

Górka, M. (2023). *The Wagner Group as a tool of Russian hybrid warfare*. https://bibliotekanauki.pl/articles/15847239

Guner, E., Iskandarov, K., & Gawliczek, P. (2022). Theories of war in practice: Causes and termination. *Wiedza Obronna*. https://yadda.icm.edu.pl

Harward, C., Evans, A., Mappes, G., Gibson, O., Kagan, F. W., & Runkel, W. (2025). *Russian offensive campaign assessment*. Institute for the Study of War. https://www.understandingwar.org

Hirose, Y. (2025). *Hybrid warfare transformed amidst the Ukraine war*. https://ssdpaki.la.coocan.jp

Hunder, M. (2026, February 27). Ukraine may form joint ventures with allies to boost defenses. *Reuters*. https://www.reuters.com

Ilyushina, M. (2025, June 1). Ukraine attacks Russian air bases in drone strikes. *The Washington Post*. https://www.washingtonpost.com

Institute of Naval Forces of Ukraine. (2023). *Forced migration as a consequence of Russia's hybrid war*. https://ivms.mil.gov.ua

IntSecurity.org. (2023). *Russia–Ukraine war newsletter (July 17–23, 2023)*. https://intsecurity.org

Iskandarov, K., & Gawliczek, P. (2020a). Early identification of threats. *Social Development and Security, 10*(4), 102–109.

Iskandarov, K., & Gawliczek, P. (2020b). Hybrid warfare as an instrument of political leverage. In M. Banasik et al. (Eds.), *The Russian Federation and international security* (pp. 117–136). Difin.

Iskandarov, K., & Gawliczek, P. (2020c). Hybrid warfare as a new type of war. In M. Banasik et al. (Eds.), *The Russian Federation and international security* (pp. 96–107). Difin.

Iskandarov, K., & Gawliczek, P. (2020d). The impact of social media on the war. In M. Banasik et al. (Eds.), *Information, media, security environment* (pp. 162–178). Difin.

Iskandarov, K., & Gawliczek, P. (2021). Deterrence as a component of response to hybrid threats. *Civitas et Lex, 29*(1), 17–26. https://doi.org/10.31648/cetl.6124

Iskandarov, K., & Gawliczek, P. (2025). Coercion through threat and use of force. *Przegląd Strategiczny, 18*, 21–35. https://pressto.amu.edu.pl

Iskandarov, K., Gawliczek, P., & Soboń, A. (2024). Violation of territorial integrity as a tool of hybrid warfare. *Security and Defence Quarterly, 45*(1), 1–17. https://doi.org/10.35467/sdq/174507

Iskandarov, K., Gawliczek, P., & Tomasik, J. (2022). Termination of war. *Civitas et Lex, 35*(3), 7–17.

Jędrysiak, M. (2024). *Ukraine: Corruption scandal over fake disability certificates*. OSW. https://www.osw.waw.pl

Jankowicz, M. (2023). Ukrainian man paid $5,000 to avoid conscription. *Business Insider*. https://www.businessinsider.com

Knutson, J. (2022). Russia has conducted hundreds of cyberattacks against Ukraine. *Axios*. https://www.axios.com

Kramer, A. (2023, August 11). Ukraine fires recruitment chiefs after corruption probe. *The New York Times*. https://www.nytimes.com

Langston, V. (2026, February 18). Russia's Doppelgänger operation. *Medium*. https://medium.com

Le Gargasson, C., & Black, J. (2025). Electromagnetic warfare. *RAND Corporation*. https://www.rand.org

Lewis, J. A. (2022). *Cyber war and Ukraine*. CSIS. https://www.csis.org

Loh, M. (2026, February 24). Ukraine uses interceptor drones. *Business Insider*. https://www.businessinsider.com

Mansoor, P. R. (2012). Introduction: Hybrid warfare in history. In W. Murray & P. Mansoor (Eds.), *Hybrid warfare*. Cambridge University Press.

Marusyak, B. (2023). Russian redeployment of special forces. https://www.promoteukraine.org

Mihaylov, N. (2025). *Cyber dimensions of hybrid warfare*. CyberPeace Institute. https://cyberpeaceinstitute.org

Ministry of Defence of Ukraine. (n.d.). *Territorial defense forces*. https://mod.gov.ua

National Security and Defense Council of Ukraine. (2025). *Center for Countering Disinformation report*. https://www.rnbo.gov.ua
Neville, S. B. (2015). *Russia and hybrid warfare* (Master's thesis). Naval Postgraduate School.
Orenstein, M. (2022). *Russia's use of cyberattacks*. FPRI. https://www.fpri.org
Petriv, O. (2024). Artificial intelligence and deepfakes. CEDEM. https://cedem.org.ua
Pusztaszeri, A., & Harding, E. (2025). *Technological evolution on the battlefield*. CSIS. https://www.csis.org
Rehan, T. (2025). AI-driven disinformation campaigns. *Small Wars Journal*.
Reuters. (2023). Russia-Ukraine war updates. https://www.reuters.com
Reuters. (2026). Russia attacked Ukraine with missiles and drones. https://www.reuters.com
Riehle, K. (2024). The Ukraine war and intelligence shift. *Intelligence and National Security, 39*(3), 458–474. https://doi.org/10.1080/02684527.2024.2322807
Riley-Smith, B. (2025). Russia targets Ukrainians through phones. *The Times*.
Romaniuk, R. (2024). Sea drones and Black Sea dominance. *Ukrainska Pravda*.
Schulze, M., & Kerttunen, M. (2023). Cyber operations in Russia's war against Ukraine. SWP.
Smith, B. (2022). Defending Ukraine. Microsoft.
Spravdi. (2023). Strategic communication report. https://spravdi.org
Takagi, K. (2023). Intelligence revolution in Ukraine war. Hudson Institute.
The Guardian. (2025). Ukraine war briefing: Anti-corruption agency in Kyiv accuses deputy PM. https://www.theguardian.com
Tyshchenko, K. (2025). Ukraine uncovers bribery scheme. *Ukrainska Pravda*.
Ukrainska Pravda. (2022). Cyber warfare statistics. https://www.pravda.com.ua
Vakulina, S. (2025). Tackling Russia's hybrid war. *Euronews*.
Welsch, M. (2025). *Ukraine air war monitor (Vol. VIII)*. Konrad-Adenauer-Stiftung.
Welsch, M. (2026). *Ukraine air war monitor (Vol. XIII)*. Kyiv Dialogue.
WiFiTalents. (2026). *Hybrid warfare statistics*. https://wifitalents.com
Yakovenko, N. L., & Piskorska, H. (2023). Hybrid war of Russia against Ukraine. *American History & Politics*.
Zarembo, K., & Solodkyy, S. (2021). *The evolution of Russian hybrid warfare: Ukraine*. CEPA.