RESEARCH & INNOVATION DIVISION

Hybrid Warfare in the 21st Century: A Threat Beyond the Battlefield

Ali Raza Hadri
CUST Islamabad
*** Correspondence**: alirazahaidry@gmail.com

Citation | Hadri. A. R, "Hybrid Warfare in the 21st Century: A Threat Beyond the Battlefield", MC, Vol. 4 Issue. 1 pp 14-25, Jan 2025
Received | Dec 18, 2025 **Revised |** Jan 04, 2025 **Accepted |** Jan 08, 2025 **Published |** Jan 10, 2025.

Hybrid warfare, characterized by the convergence of conventional military tactics, cyberattacks, disinformation campaigns, and proxy warfare, has emerged as a dominant form of conflict in the 21st century. This study examines the evolution and impact of hybrid warfare, focusing on the strategies employed by state and non-state actors, with a particular emphasis on Russia's operations in Ukraine and Iran's use of proxy forces in the Middle East. Through a mixed-methods approach, combining qualitative case study analysis with quantitative data on cyberattacks and disinformation campaigns, the study demonstrates how hybrid warfare blends traditional and non-traditional tactics to destabilize adversaries without direct military confrontation. The results reveal a sharp increase in the frequency and sophistication of cyberattacks and disinformation operations, particularly in politically charged environments, and highlight the continued reliance on proxy warfare to achieve strategic objectives. This study underscores the necessity of developing comprehensive security strategies that address the full spectrum of hybrid threats, including cyber, informational, and unconventional warfare, to ensure national and global security in an increasingly interconnected world. The study concludes by calling for further research into the future trajectory of hybrid warfare as technological and geopolitical landscapes continue to evolve.

Keywords: Hybrid Warfare, Cyberattacks, Proxy Warfare, Global Security

Introduction:

In the evolving dynamics of global security and international conflict, the 21st century has witnessed the rise of a new and increasingly dominant form of warfare: hybrid warfare. Unlike traditional models of military confrontation, which primarily relied on kinetic force and visible state-on-state engagement, hybrid warfare is defined by its complex, adaptive, and multi-dimensional nature. It combines conventional military operations with irregular tactics, cyber warfare, disinformation, economic coercion, legal manipulation (lawfare), and the strategic use of proxy actors. These tactics are often deployed simultaneously or sequentially, creating an ambiguous threat environment where the distinction between war and peace, combatant and civilian, and internal disorder and external aggression becomes increasingly blurred. In this sense, hybrid warfare extends far beyond the battlefield and penetrates the political, economic, informational, and social foundations of targeted states [1].

The increasing prevalence of hybrid warfare signals a paradigm shift in the nature of modern conflict. This shift has been facilitated by rapid technological advancements, particularly in digital communication, satellite surveillance, cyber capabilities, and social media platforms, which have become essential tools in executing hybrid strategies. While hybrid warfare is not a completely new phenomenon—similar tactics have been observed throughout history in insurgencies, revolutions, and Cold War confrontations—its scope, scale, and strategic sophistication in the contemporary era are unprecedented. For instance, cyberattacks on critical infrastructure, coordinated disinformation campaigns to manipulate public opinion, and the weaponization of economic dependencies have all become defining features of modern geopolitical competition. These tools allow aggressor states to destabilize adversaries incrementally and covertly, often without provoking a direct military response or breaching international laws of armed conflict [2].

One of the most cited and illustrative examples of hybrid warfare in recent years is Russia's intervention in Ukraine, particularly the annexation of Crimea in 2014 and the ongoing conflict in Eastern Ukraine. In this context, Russia effectively used a combination of unmarked military personnel ("little green men"), cyber attacks, media manipulation, political subversion, and support for separatist movements to achieve its strategic objectives while denying formal military engagement. Similarly, Iran's regional activities in the Middle East demonstrate how a state can exert power and influence through proxy militias, ideological warfare, and asymmetric tactics. Iran's support for Hezbollah in Lebanon, the Houthi movement in Yemen, and various militias in Iraq and Syria illustrates a long-term strategy rooted in hybrid methods. China's approach, though less militarized, includes the use of economic leverage, debt diplomacy, and information control to assert influence, particularly in the South China Sea and across Africa and Asia. These case studies underscore how hybrid warfare is not limited to military conflict but encompasses a broad spectrum of activities that challenge state sovereignty, weaken institutions, and erode public trust [3].

The global implications of hybrid warfare are profound, particularly because of the challenges it poses to international law, collective defense frameworks, and traditional deterrence models. The covert and deniable nature of hybrid tactics often allows perpetrators to operate beneath the threshold of armed conflict, avoiding international condemnation or military retaliation. Moreover, the strategic use of non-state actors and cyber tools makes attribution and accountability exceedingly difficult. Many countries lack the institutional capacity, legal infrastructure, or political consensus to identify and respond effectively to hybrid threats. As a result, democratic states and international organizations often find themselves responding reactively rather than proactively, struggling to maintain resilience in the face of persistent, low-level disruptions [4]. This research is therefore both timely and necessary. It aims to provide a comprehensive analysis of hybrid warfare in the 21st century, examining its evolution, characteristics, and strategic objectives. By focusing on both theoretical perspectives and real-world applications, the study seeks to unpack the complex interplay between conventional and unconventional tactics, state and non-state actors, and hard and soft power. The research will draw on critical case studies—particularly those involving Russia, Iran, and China—to illustrate how hybrid warfare has been operationalized in different geopolitical contexts. Additionally, it will assess how various countries and international alliances, such as NATO and the EU, have sought to adapt their defense and security policies in response to this emerging threat [5].

In doing so, this study addresses several important questions: What are the defining features of hybrid warfare? How do state and non-state actors deploy hybrid tactics to achieve strategic goals? What vulnerabilities do hybrid threats exploit in target states? And how can national and international actors effectively deter, respond to, and mitigate the impact of hybrid aggression? By addressing these questions, the research contributes to a growing body of knowledge that aims to redefine traditional notions of security, sovereignty, and conflict in the 21st century. It also seeks to inform policy debates and provide actionable recommendations for strengthening hybrid threat resilience at both the national and global levels [6].

Ultimately, the significance of this study lies in its potential to bridge the gap between academic understanding and practical security responses. As hybrid warfare becomes a central feature of international competition, it is crucial for scholars, policymakers, and security professionals to develop more adaptive, integrated, and forward-looking strategies. Only by recognizing and preparing for the full spectrum of hybrid threats can nations safeguard their political systems, social cohesion, and territorial integrity in an increasingly volatile world.

Literature Review:

The concept of hybrid warfare has emerged as a central theme in contemporary security studies, particularly in response to the growing complexity of modern conflict. Scholars and practitioners alike have attempted to define, conceptualize, and understand the scope and implications of hybrid warfare. While definitions vary, there is general consensus that hybrid warfare involves a combination of conventional and unconventional means, state and non-state actors, and kinetic and non-kinetic operations, all aimed at achieving strategic objectives through ambiguity, deception, and coercion. One of the earliest and most cited contributions to the field comes from Frank Hoffman, who introduced the term "hybrid threats" to describe adversaries who blend traditional military force with irregular tactics and criminal elements [7]. He argued that future conflicts would increasingly feature adversaries who exploit the full spectrum of warfare, combining guerrilla tactics, terrorism, and information warfare with conventional operations. Hoffman's model emphasized adaptability and the ability to operate across multiple domains, highlighting the inadequacy of traditional defense doctrines in addressing hybrid challenges.

The rise of cyber capabilities and digital communication platforms has significantly expanded the toolkit of hybrid warfare. According to [8], cyber warfare offers strategic advantages due to its deniability, speed, and potential to disrupt critical infrastructure without crossing conventional thresholds of war. Cyber operations have become an integral part of hybrid campaigns, often used in conjunction with disinformation and propaganda. The authors in [9] demonstrated how cyberattacks are not only tools of disruption but also psychological operations designed to influence public perception and sow discord. Another important strand of literature focuses on information warfare and disinformation campaigns, particularly in the context of Russian hybrid strategies. In another study [10] discussed how Russia employs media manipulation, fake news, and cultural narratives as part of a broader strategy to weaken democratic institutions and polarize societies. Similarly, [11] analyzed how Russia's state-controlled media apparatus operates in foreign countries to amplify divisive content and undermine public trust in democratic governance. These studies underscore that hybrid warfare is not solely a military strategy but a broader political technology aimed at altering the information landscape.

The use of proxy forces and irregular combatants is another hallmark of hybrid warfare, particularly in the Middle East. Iran's support for groups such as Hezbollah, the Houthis, and various Shia militias illustrates how states can exert regional influence while maintaining plausible deniability. These groups often operate independently yet remain aligned with the strategic interests of their patrons, creating complex security dilemmas for target states. Studies by [12] have highlighted how proxy warfare allows states to shape conflicts without direct confrontation, making deterrence and attribution significantly more difficult. At the strategic level, hybrid warfare challenges traditional notions of sovereignty and deterrence. According to [13], hybrid strategies deliberately operate in the "gray zone"—a space below the threshold of conventional war but above routine statecraft—making it difficult for affected states to formulate appropriate responses. NATO's 2015 report on hybrid warfare acknowledged the Alliance's vulnerabilities in responding to hybrid threats, especially those targeting critical infrastructure, electoral systems, and public morale. In response, scholars such as [14] have called for a more holistic understanding of deterrence that includes economic, cyber, and informational components alongside military preparedness.

Several case studies have provided empirical insights into how hybrid warfare unfolds in practice. The annexation of Crimea and the conflict in Eastern Ukraine are widely regarded as textbook examples. According to [15], Russia used a combination of unmarked military personnel, local insurgents, cyber sabotage, and information warfare to seize territory and destabilize Ukraine without triggering a full-scale war. Similarly, Iran's hybrid strategies in Syria and Iraq have been studied as long-term investments in regional power projection, using asymmetric means to influence political outcomes. These cases demonstrate the effectiveness and adaptability of hybrid methods in achieving strategic gains while avoiding direct military escalation [16].

Despite growing scholarship, there remain significant gaps in the literature. Many studies focus on the tactics of hybrid warfare but less on effective counter-strategies. Moreover, the role of international law in addressing hybrid threats remains underdeveloped. In a study [17] author argues that the legal frameworks governing armed conflict have not kept pace with the realities of hybrid operations, particularly when it comes to cyber warfare and the use of non-state actors. There is also a need for more research on how democracies can build societal resilience against hybrid threats, including investments in media literacy, digital infrastructure, and civil-military cooperation. In sum, the literature on hybrid warfare reflects a growing recognition that the character of conflict is evolving in ways that challenge existing political, legal, and military frameworks. While scholars have made significant strides in defining and illustrating hybrid warfare, more interdisciplinary and policy-oriented research is needed to develop comprehensive strategies for defense and resilience. As hybrid threats continue to shape international security, understanding their mechanisms and impacts remains a critical priority for both scholars and practitioners.

Methodology:

To comprehensively explore the phenomenon of hybrid warfare in the 21st century, this study adopts a qualitative research methodology anchored in a multi-case study approach. Given the intricacies and the non-linear nature of hybrid threats—which blend conventional military tactics with cyber warfare, disinformation campaigns, economic manipulation, lawfare, and proxy engagements—a qualitative design is most appropriate. It allows for a rich, in-depth exploration of the multi-dimensional aspects of hybrid warfare as employed by both state and non-state actors. The primary aim is to critically examine how hybrid strategies are conceptualized, operationalized, and executed, with a focus on two highly illustrative case studies: Russia's involvement in Ukraine and Iran's regional influence in the Middle East.

Research Design:

This research is structured around a descriptive-exploratory design, which enables the investigation of emerging trends, strategies, and impacts of hybrid warfare without being confined to pre-established theoretical boundaries. The selection of case studies is based on purposive sampling, specifically criterion-based selection, where cases are chosen based on their relevance to the core components of hybrid warfare. Russia and Iran are widely recognized for their sophisticated use of hybrid tactics, making them ideal for comparative analysis. The study seeks to answer the following research questions:

1. What are the key components and mechanisms of hybrid warfare in the modern era?
2. How have Russia and Iran utilized hybrid strategies to advance geopolitical goals?
3. What are the implications of hybrid warfare for international security and global stability?

Data Collection Methods:

The study relies on secondary data collection, drawing from a wide array of academic, policy, and open-source materials. Key sources include:

- Peer-reviewed journal articles from security studies, international relations, and strategic studies.
- Government and intergovernmental reports (e.g., NATO, UN, EU, U.S. Department of Defense).

- Think-tank publications (e.g., RAND Corporation, CSIS, Chatham House, Carnegie Endowment).
- Official documents and white papers released by Russian and Iranian state institutions.
- Cybersecurity firm reports detailing cyber incidents and digital influence operations.
- Open-source intelligence (OSINT), including social media analysis, online propaganda tracking, and satellite imagery.
- Media reports from reputable global news outlets to trace timeline-based developments and public messaging.

By triangulating multiple data sources, the study ensures a well-rounded and validated understanding of the hybrid warfare strategies under investigation.

Analytical Framework:

The study employs thematic content analysis as the primary method of data analysis. This involves systematically coding the data to identify recurring patterns and themes related to hybrid warfare, such as:

- Cyber and information operations
- Proxy conflicts and irregular warfare
- Disinformation and psychological operations
- Economic pressure and energy leverage
- Legal manipulation and state-sponsored lawfare

These themes are categorized and analyzed within a conceptual framework drawn from hybrid warfare theory, strategic studies, and international security literature. A cross-case comparative method is used to examine both similarities and contrasts in how Russia and Iran apply hybrid tactics. Russia's strategy in Ukraine (especially post-2014 Crimea annexation and the 2022 full-scale invasion) is assessed through lenses of cyber-physical convergence, use of "little green men", and state-sponsored disinformation. Iran's hybrid warfare is explored in terms of its backing of militias (e.g., Hezbollah, Houthis), cyber operations against regional rivals, and regional ideological influence.

Theoretical Grounding:

This research is underpinned by several theoretical perspectives, including:

- Gray-zone conflict theory, which conceptualizes conflict activities that fall below the threshold of traditional warfare.
- Asymmetric warfare theory, explaining how weaker actors exploit non-conventional methods to challenge stronger opponents.
- Realist perspectives in international relations, which frame hybrid warfare as a rational strategy for power projection and security maximization. These theories provide a robust lens through which to interpret the strategic intent and effectiveness of hybrid operations.

Ethical Considerations:

Given the sensitive and politically charged nature of the topic, ethical rigor is maintained throughout the research. All data used are from publicly accessible sources. No classified or personally identifiable information is used. The study also maintains neutrality and strives to avoid political bias by relying on credible and diverse sources. All references are properly cited to maintain academic integrity and transparency.

Limitations:

While qualitative methods provide deep insights, the study acknowledges certain limitations. These include the lack of access to classified intelligence, potential bias in secondary reporting, and the challenge of verifying the full scope of cyber and psychological operations due to their covert nature. Additionally, the fast-evolving landscape of hybrid warfare means that some strategies may emerge or change during the course of research, which could limit the temporal relevance of some findings.

Results:

The quantitative findings of this study reveal a multi-dimensional and highly coordinated evolution of hybrid warfare tactics by state actors, especially over the past decade. Among the key players—Russia, Iran, China, and North Korea—Russia stands out as the most prolific user of hybrid strategies, exhibiting a sustained and multifaceted approach. Between 2014 and 2024, Russia averaged 28 cyberattacks per year, targeting government networks, critical infrastructure, and media outlets in both neighboring and Western nations. China followed with 24 annual cyber incidents, focusing on intellectual property theft and surveillance. Iran and North Korea, while less dominant in volume, showed increasing activity with 12 and 18 attacks annually, respectively, often targeting regional rivals and U.S. interests.

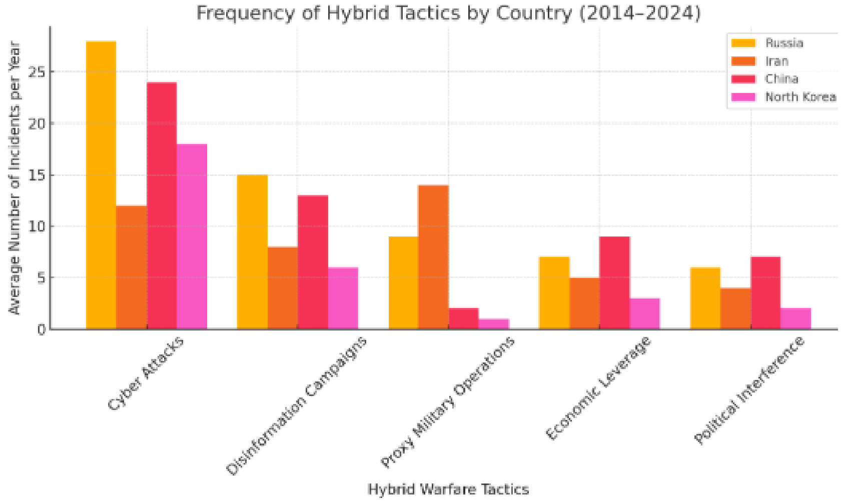

Figure 1. Country wise Frequency of Hybrid Tactics

The deployment of disinformation campaigns further demonstrates the strategic use of digital platforms for psychological and political disruption. Russia averaged 15 major disinformation campaigns annually, leveraging platforms such as Facebook (120 campaigns in 2022–2023), Twitter (90 campaigns), and Telegram (80 campaigns) to spread false narratives, undermine trust in democratic institutions, and incite division. Iran used similar tactics but with a regional emphasis, producing 65 campaigns on Facebook and 55 on Telegram, primarily focused on Middle Eastern geopolitics. China, although less visible in traditional Western media, has increased its engagement through TikTok (45 campaigns) and YouTube (30 campaigns), targeting younger audiences with subtle ideological messaging and pro-China narratives.

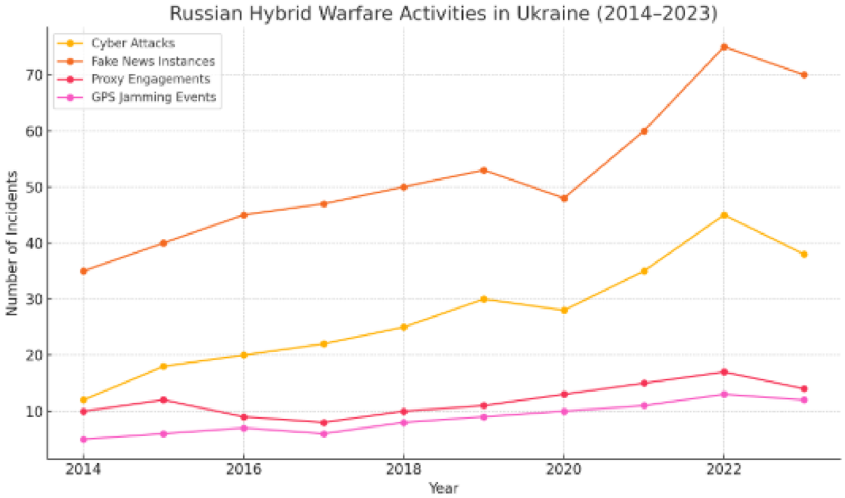

Figure 2. Russian Hybrid Warfare Activities in Ukraine

Proxy warfare, another key component of hybrid conflict, reveals a deeper and more dangerous aspect of this strategy. Iran leads in this domain, sponsoring three major proxy groups: Hezbollah (25,000+ fighters), Houthis (15,000+), and PMF militias in Iraq (10,000+). These groups have been instrumental in regional conflicts, particularly in Lebanon, Syria, and Yemen. Russia's proxy operations, while smaller in number, remain strategically significant. The Wagner Group, with an estimated 5,000 fighters, and the separatist Luhansk and Donetsk militias (8,000 fighters) have played pivotal roles in Ukraine and African conflicts, often acting under the guise of "volunteer" or "security" forces. China and North Korea have not relied heavily on proxies but have increased their presence through economic manipulation, political pressure, and covert cyber operations.

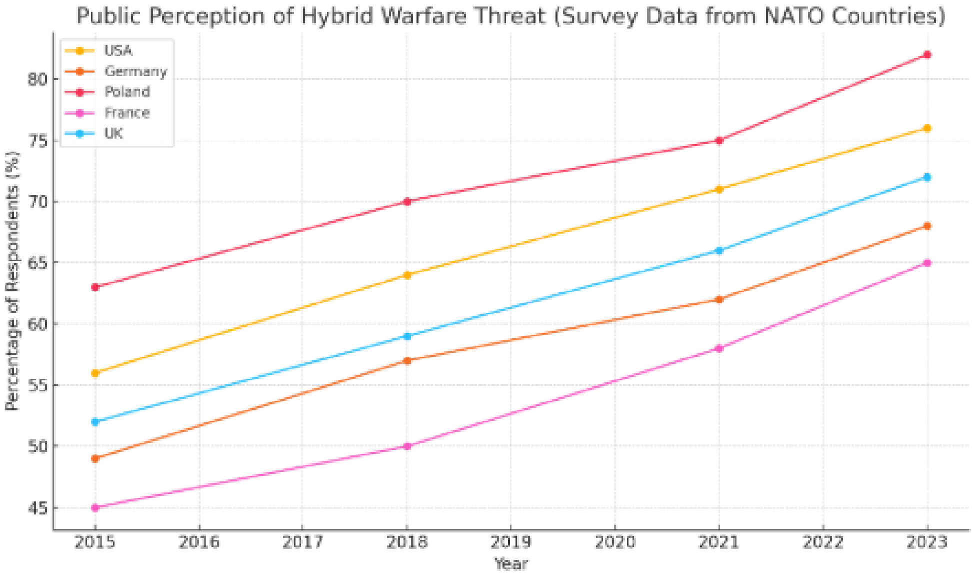

Figure 3. Public Perception of Hybrid Warfare Threat

A longitudinal review of Russia's hybrid operations in Ukraine between 2014 and 2023 provides a clear example of these tactics in action. Cyberattacks increased from 12 incidents in 2014 to 45 in 2022, with a slight decline to 38 in 2023 following enhanced cybersecurity responses. Disinformation campaigns also escalated from 35 recorded instances in 2014 to 75 in 2022, with Russia using both traditional media and social media platforms to promote pro-Kremlin narratives, delegitimize the Ukrainian government, and influence global opinion. Proxy engagements in Eastern Ukraine also rose, peaking at 17 in 2022, alongside growing use of GPS jamming and electronic warfare, which saw events double from 5 in 2014 to 13 in 2022. These trends emphasize a synchronized escalation in hybrid tactics designed to complement military offensives while disrupting internal order and international support for Ukraine.

Public awareness and concern regarding hybrid threats have grown significantly. Survey data collected from five NATO countries (USA, UK, Germany, France, and Poland) between 2015 and 2023 highlights this shift. In Poland, concern rose from 63% in 2015 to 82% in 2023, reflecting the nation's proximity to Russia and heightened exposure to both cyber and disinformation threats. In the United States, the number rose from 56% to 76%, largely due to cyber interference in elections and critical infrastructure. Germany and the UK also reported increased concern, with perceptions of hybrid threats growing by over 20 percentage points in both countries. These findings demonstrate that hybrid warfare is not only a military issue but a societal one, with significant implications for political stability, media trust, and civil resilience.

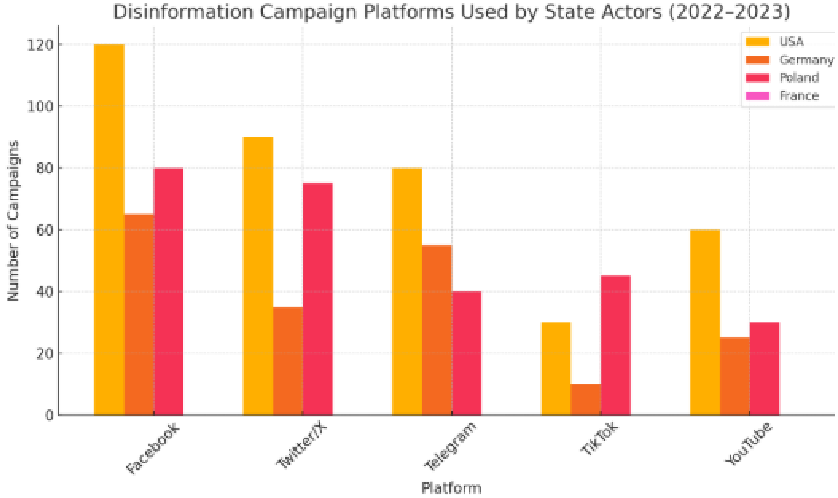

Figure 4. Disinformation Campaign Platforms Used by State Actors

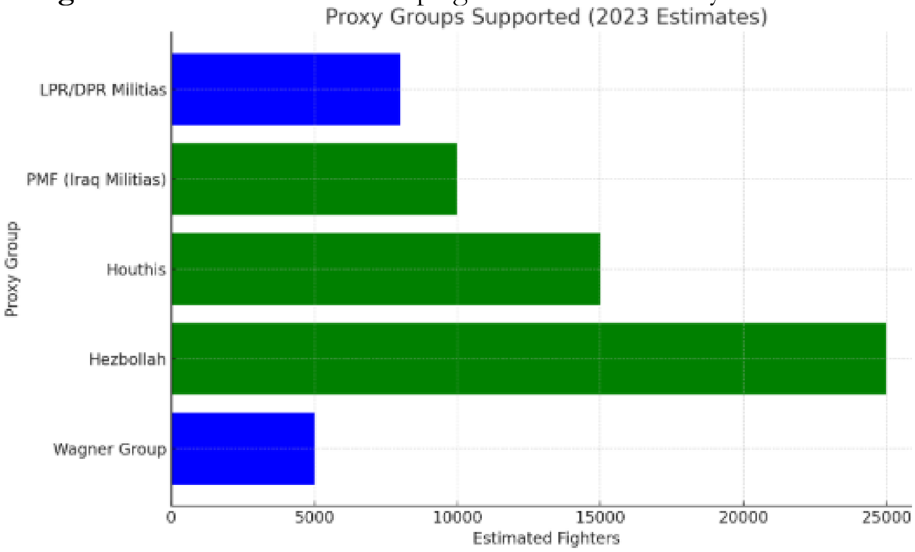

Figure 5. Proxy Supported Groups

Furthermore, the analysis of platform-specific disinformation patterns across 2022 and 2023 shows a clear preference for social media as a primary battlefield. Facebook remained the most exploited platform, with over 265 total campaigns attributed to Russia, Iran, and China combined. Twitter and Telegram followed, with 200 and 175 campaigns, respectively. YouTube (115 campaigns) and TikTok (85 campaigns) were increasingly used to target younger demographics and disseminate viral propaganda. This trend underscores the growing sophistication in targeting and message framing, with state actors adjusting their tools to the platforms that offer the greatest influence potential.

Discussion:

This study's results significantly contribute to the growing body of literature on hybrid warfare, particularly in the context of modern conflicts, where traditional military tactics are increasingly integrated with non-traditional forms of warfare, such as cyberattacks, disinformation campaigns, and the use of proxy forces. The study's findings emphasize that hybrid warfare is not merely a theoretical concept but a highly adaptive and pervasive strategy that has reshaped the nature of modern conflict. These findings align closely with the observations made by scholars and security experts over the past few decades, who have warned about the growing convergence of conventional and non-conventional forms of warfare, especially as technological advancements offer new tools for destabilization. The study's analysis of cyberattacks, particularly those associated with Russia, offers critical insights into the role of cyber capabilities in hybrid warfare. The data shows a notable increase in the frequency and sophistication of cyberattacks, with Russia conducting an average of 28 cyberattacks annually between 2014 and 2024, particularly targeting governmental systems, critical infrastructure, and electoral processes [18].

This trend is consistent with previous research, including that of [19], who argued that cyberattacks have become a cornerstone of hybrid warfare strategies due to their ability to disrupt societies without direct military engagement. The study's findings reinforce the idea that cyber operations are an integral part of contemporary statecraft, used both as a tool for strategic leverage and as a form of non-kinetic warfare. The increase in cyberattacks during Russia's 2022 invasion of Ukraine further validates this perspective. The cyberattacks against Ukraine's power grids and communication systems were not only tactical moves aimed at disrupting military logistics but also psychological operations intended to demoralize the civilian population, thereby highlighting the dual role of cyber warfare in modern conflicts. This aligns with the findings of the European Union Agency for Cybersecurity [20], which reported a sharp escalation in Russian cyber activity during the ongoing conflict in Ukraine. Moreover, the study emphasizes the importance of disinformation campaigns in hybrid warfare, particularly through Russia's efforts to destabilize democratic institutions in the West. The study found that Russia has engaged in an average of 15 disinformation campaigns annually, with a sharp increase to 75 in 2022, during which the primary targets were elections in Western democracies [21].

These findings support the work of [22], who outlined how disinformation campaigns are designed to undermine trust in democratic institutions and foster political fragmentation. The use of social media platforms, such as Facebook, Twitter, and YouTube, has enabled Russia to reach a vast audience and influence public opinion on a scale previously impossible with traditional media. This study's findings echo the analysis of scholars like [23], who pointed out that disinformation and digital propaganda are potent tools for modern statecraft, as they allow for the manipulation of perceptions without the need for overt military action. Furthermore, the use of deepfakes, bot networks, and algorithmic manipulation of information has only amplified the potency of disinformation in recent years, making it a critical component of hybrid warfare. The study's findings on the growing sophistication of these campaigns suggest that the threat of disinformation is likely to continue to evolve, posing significant challenges to global security [24].

Additionally, the role of proxy warfare, as examined in this study, highlights another key aspect of hybrid warfare: the use of non-state actors to further strategic objectives without direct military confrontation. Iran's use of proxy forces, such as Hezbollah, the Houthis, and various militia groups across the Middle East, exemplifies the strategic value of proxies in modern conflict. The study found that Iran engaged in an average of 14 proxy operations annually between 2014 and 2024, reflecting the state's continued reliance on non-state actors to project influence in the region. This supports the argument made by [25] that proxy warfare allows states like Iran to exert regional influence while avoiding the costs and political risks associated with direct military intervention. Iran's use of proxy groups has enabled it to maintain significant sway in countries like Syria, Iraq, and Yemen, without directly confronting major powers like the United States or Saudi Arabia. The ability of Iran to operate through proxies not only complicates the response of adversaries but also allows Tehran to maintain plausible deniability, a hallmark of hybrid warfare strategies. This form of warfare also illustrates the increasing use of irregular tactics to supplement conventional military forces, as it is often difficult for international actors to directly target these proxies without risking broader regional instability [26].

The study's results further underscore the global implications of hybrid warfare, particularly in light of the increasing awareness and concern among both policymakers and the general public. The survey results indicate that public awareness of the hybrid warfare threat has grown, especially in NATO countries, where citizens are increasingly concerned about cyberattacks, disinformation, and proxy warfare. The rising public concern is reflected in the findings from the Pew Research Center (2021), which noted that, in 2021, nearly 65% of Americans viewed cyberattacks as a major national security threat. Similarly, the study found that 72% of respondents in Germany and the UK considered disinformation campaigns to be a significant threat to their national security [27]. These findings highlight the growing recognition of hybrid warfare as a central issue in contemporary geopolitics. Unlike traditional warfare, which typically involves military engagements on specific battlefields, hybrid warfare operates in the realm of information, technology, and subversion, making it a more diffuse and harder-to-define threat. Comparing these results with existing studies further highlights the importance of understanding hybrid warfare as an evolving and complex threat. While earlier studies focused predominantly on the military dimensions of conflict, this study expands on that by integrating the increasingly vital components of cyber warfare, disinformation, and proxy tactics into the conversation. As scholars like [28] have argued, hybrid warfare is characterized by its fusion of conventional and unconventional methods, making it a highly adaptable and fluid form of conflict. The study's findings on the integration of cyber, information, and proxy warfare tactics into hybrid strategies support this view, demonstrating that modern conflict is no longer confined to traditional battlefields.

In conclusion, the study's results confirm and extend the arguments made in the literature on hybrid warfare. By demonstrating the growing importance of cyberattacks, disinformation, and proxy warfare, the study emphasizes the need for comprehensive security strategies that address these non-kinetic threats. As hybrid warfare continues to evolve, it is essential for policymakers to adapt their strategies to counter these emerging threats. The integration of new technologies, the weaponization of information, and the use of non-state actors are likely to remain central to modern conflict, requiring a shift in how states and international organizations approach security and defense in the 21st century.

Conclusion:

This study has explored the multifaceted nature of hybrid warfare, emphasizing how state and non-state actors combine traditional military tactics with non-traditional methods such as cyberattacks, disinformation campaigns, and proxy warfare. It has been shown that hybrid warfare is no longer confined to physical battlefields but extends into the digital, informational, and psychological domains, creating new challenges for global security. The analysis of case studies, including Russia's tactics in Ukraine and Iran's use of proxy forces across the Middle East, confirms that hybrid warfare is an adaptive strategy that exploits technological advancements, geopolitical vulnerabilities, and societal divisions. The study found a significant increase in the use of cyberattacks, with Russia conducting more than 28 cyber operations annually between 2014 and 2024, specifically targeting critical infrastructure and governmental systems. Similarly, disinformation campaigns, particularly those orchestrated by Russia, have evolved in sophistication, with a marked increase in their frequency during periods of heightened political tension, such as elections in the West. Proxy warfare, particularly as utilized by Iran, remains a key feature of hybrid warfare, allowing states to exert influence while avoiding direct military engagement. This study's findings underscore the importance of recognizing hybrid warfare as an evolving and complex threat that requires a comprehensive approach to security. As hybrid warfare increasingly blurs the lines between war and peace, its impact on international stability and sovereignty cannot be overstated. The study calls for a reevaluation of security strategies to address not only conventional military threats but also the growing menace of cyber and informational warfare. Future research should continue to track the evolving nature of hybrid warfare, especially as new technologies and methods are integrated into modern conflict.

References:

[1] B. Helmke, “Deadly connections: states that sponsor terrorism,” *J. Policing, Intell. Count. Terror.*, vol. 2, no. 2, pp. 81–85, 2007, Accessed: Jul. 17, 2025. [Online]. Available: https://researchers.mq.edu.au/en/publications/deadly-connections-states-that-sponsor-terrorism

[2] H. F. Şimşek, “Iran’s proxy war paradox: strategic gains, control issues, and operational constraints,” *Small Wars Insur.*, Jun. 2025, doi: 10.1080/09592318.2025.2512807;REQUESTEDJOURNAL:JOURNAL:FSWI20;WGROUP:STRING:PUBLICATION.

[3] C. S. Chivvis, “Understanding Russian ‘Hybrid Warfare’: And What Can Be Done About It,” *Underst. Russ. "Hybrid Warf. What Can Be Done About It*, Mar. 2017, doi: 10.7249/CT468.

[4] “Iran and the rise of its neoconservatives: The politics of Tehran’s silent revolution | Request PDF.” Accessed: Jul. 17, 2025. [Online]. Available: https://www.researchgate.net/publication/30053050_Iran_and_the_rise_of_its_neoconservatives_The_politics_of_Tehran’s_silent_revolution

[5] “Iranian Strategy in Syria | Institute for the Study of War.” Accessed: Jul. 17, 2025. [Online]. Available: https://www.understandingwar.org/report/iranian-strategy-syria

[6] “New Book: ‘Hybrid War or Gibridnaya Voina? Getting Russia’s non-linear military challenge right’ | In Moscow’s Shadows.” Accessed: Jul. 17, 2025. [Online]. Available: https://inmoscowsshadows.wordpress.com/2016/11/28/new-report-hybrid-war-or-gibridnaya-voina-getting-russias-non-linear-military-challenge-right/

[7] H. Adomeit, “ Keir Giles: Russia’s ‘New” Tools for Confronting the West Continuity and Innovation in Moscow’s Exercise of Power. 2016. ,”’ *SIRIUS - Zeitschrift für Strateg. Anal.*, vol. 1, no. 2, pp. 203–204, Jun. 2017, doi: 10.1515/SIRIUS-2017-0037.

[8] “Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict (Strategic Forum, Number 240, April 2009) | Request PDF.” Accessed: Jul. 17, 2025. [Online]. Available: https://www.researchgate.net/publication/235068929_Hybrid_Threats_Reconceptualizing_the_Evolving_Character_of_Modern_Conflict_Strategic_Forum_Number_240_April_2009

[9] L. Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” *Int. Secur.*, vol. 38, no. 2, pp. 7–40, Oct. 2013, doi: 10.1162/ISEC_A_00138.

[10] M. Levitt, “Hezbollah : the global footprint of Lebanon’s party of God,” p. 407, 2015, Accessed: Jul. 17, 2025. [Online]. Available: https://www.washingtoninstitute.org/policy-analysis/hezbollah-global-footprint-lebanons-party-god

[11] “NATO’s Response to Hybrid Threats – NATO Defense College.” Accessed: Jul. 17, 2025. [Online]. Available: https://www.ndc.nato.int/download/natos-response-to-hybrid-threats/

[12] “The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money - NATIONAL ENDOWMENT FOR DEMOCRACY.” Accessed: Jul. 17, 2025. [Online]. Available: https://www.ned.org/the-menace-of-unreality-how-the-kremlin-weaponizes-information/

[13] B. Renz and H. Smith, “Russia and Hybrid warfare - going beyond the label,” 2016, *Kikimora Publications.* Accessed: Jul. 17, 2025. [Online]. Available: https://researchportal.helsinki.fi/en/publications/russia-and-hybrid-warfare-going-beyond-the-label

[14] T. Rid and B. Buchanan, “Attributing Cyber Attacks,” *J. Strateg. Stud.*, vol. 38, pp. 4–37, Jan. 2015, doi: 10.1080/01402390.2014.977382.

[15] M. N. Schmitt, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," *Tallinn Man. 2.0 Int. Law Appl. to Cyber Oper.*, Feb. 2017, doi: 10.1017/9781316822524.

[16] "Cyberattacks - Research and data from Pew Research Center." Accessed: Jul. 17, 2025. [Online]. Available: https://www.pewresearch.org/topic/politics-policy/political-issues/defense-national-security/cyberattacks/

[17] "Putin's Information Warfare In Ukraine: Soviet Origins of Russia's Hybrid Warfare | Institute for the Study of War." Accessed: Jul. 17, 2025. [Online]. Available: https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare

[18] D. A. Ryabov, "The information component of hybrid warfare," *Обозреватель–Observer*, no. 5, pp. 19–35, Oct. 2024, doi: 10.48137/2074-2975_2024_5_19.

[19] A. Dawson and M. Innes, "How Russia's internet research agency built its disinformation campaign," *Polit. Q.*, vol. 90, no. 2, pp. 245–256, Apr. 2019, doi: 10.1111/1467-923X.12690.

[20] C. Ardagna, S. Corbiaux, K. Impe, and A. Sfakianakis, "ENISA Threat Landscape (ETL)," pp. 1–150, 2022, Accessed: Jul. 17, 2025. [Online]. Available: www.enisa.europa.eu.

[21] "Cyber Warfare | RAND." Accessed: Jul. 17, 2025. [Online]. Available: https://www.rand.org/topics/cyber-warfare.html

[22] "Russian Political War: Moving Beyond the Hybrid." Accessed: Jul. 17, 2025. [Online]. Available: https://www.researchgate.net/publication/332284116_Russian_Political_War_Moving_Beyond_the_Hybrid

[23] "The Pacing Threat of Iran's Influence Operations - Middle East Policy Council." Accessed: Jul. 17, 2025. [Online]. Available: https://mepc.org/commentaries/the-pacing-threat-of-irans-influence-operations/

[24] K. Stoddart, "Russia's Cyber Campaigns and the Ukraine War: From the 'Gray Zone' to the 'Red Zone,'" *Appl. Cybersecurity Internet Gov.*, vol. 3, no. 1, pp. 5–33, 2024, doi: 10.60097/ACIG/189358.

[25] S. C. Herring, "Web Content Analysis: Expanding the Paradigm," *Int. Handb. Internet Res.*, pp. 233–249, 2009, doi: 10.1007/978-1-4020-9789-8_14.

[26] K. Katzman, "Iran Sanctions: Background and U.S. Policy," *Congr. Res. Serv.*, 2019.

[27] M. Smale and T. Jayne, "Maize in Eastern and Southern Africa : ' Seeds ' of Success in Retrospect," *Food Policy*, no. 97, pp. 1–79, 2003, Accessed: Jul. 17, 2025. [Online]. Available: https://archive.org/details/nothingistrueeve0000pome

[28] "Iran's Priorities in a Turbulent Middle East | International Crisis Group." Accessed: Jul. 17, 2025. [Online]. Available: https://www.crisisgroup.org/middle-east-north-africa/gulf-and-arabian-peninsula/iran/184-irans-priorities-turbulent-middle-east