SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 02 No. 03 (2025), pp. 262-273
Research Article
doi: https://doi.org/10.70710/sitj.v2i3.63

Intelligence Failures in the Asymmetric War between Ukraine and Russia: A Literature Review of Ukraine's Drone Attacks on Russian Military Infrastructure

Tarsito Ito[1,a,*]

[1]University of Indonesia, Jakarta
[a]asepcakwi@gmail.com
*Corresponding author

Article Info
Received: 17-June-2025
Revised: 30-Aug-2025
Published: 8-Sept-2025

Keywords
Asymmetric Warfare; Intelligence Failures; Russia; Ukraine

Abstract
The asymmetric war between Ukraine and Russia since the Russian invasion in February 2022 has demonstrated a major transformation in the conduct of modern warfare. This study focuses on analyzing Russia's intelligence failures in responding to Ukraine's drone attacks on Russian military infrastructure. Despite its limited conventional military resources, Ukraine has successfully employed tactical strategies by utilizing low-cost yet effective drone technology, including First-Person View (FPV) and modified commercial drones. These attacks have damaged Russia's strategic targets and exposed structural vulnerabilities in Russia's defense and intelligence systems. This research explores how Russia's intelligence system, which relies on hierarchical and conventional approaches, has failed to adequately prepare for new threats posed by lightweight, flexible technologies. Using a qualitative literature review method, this study identifies that shifting toward low-tech warfare and systemic disruption requires profound reforms in Russia's intelligence structure and defense system. These findings are relevant in the military context and provide important insights for resource-constrained countries in designing more adaptive defense strategies against asymmetric threats in the 21st century.

1. Introduction

As a socio-political phenomenon, war has undergone significant evolution alongside technological advances and changes in the global geopolitical landscape. While conventional battles between major military powers largely defined 20th-century warfare, the 21st century has shifted toward more asymmetric, adaptive, and technology-driven forms of conflict. This new paradigm, known as asymmetric warfare, occurs when a militarily weaker party uses unconventional strategies to counterbalance or undermine a superior force.

Two main factors drive this change. First, the revolution in information and communication technologies has facilitated the spread of inexpensive and easily accessible weapon systems, including drones, cyber tools, and remote-control systems. Second, the contemporary geopolitical landscape shows that conflicts often do not occur between two equally powerful states but frequently involve state and non-state actors, separatist groups, or smaller countries facing the military dominance of an opponent.

The use of drones by non-state armed groups such as Hezbollah, the Houthis, and militias in the Middle East over the past decade illustrates how warfare has become more decentralized and unpredictable. This highlights the vulnerability of conventional defense systems, which are designed to counter large-scale threats but struggle against fragmented, rapid, and technologically disruptive attacks. Understanding modern, non-conventional warfare's characteristics is crucial for developing strategic responses and relevant defense policies.

Russia's invasion of Ukraine in February 2022 represents a pivotal turning point in modern military conflict. Russia, as one of the world's largest military powers, launched a full-scale military operation under the assumption that its superiority in weaponry and manpower would swiftly subdue Ukraine. However, this assumption proved wrong. Ukraine demonstrated unexpected resilience through the adoption of effective unconventional strategies, including the use of light weapons, civilian mobilization, cyber attacks, and, notably, drone operations targeting strategic objectives. The fundamental difference in military approaches between the two countries underscores the nature of the ongoing asymmetric war. Russia relies on a conventional, hierarchical, centralized military doctrine, prioritizing air power, heavy artillery, and extensive logistics. In contrast, Ukraine, aware of its limitations, chose a disruptive strategy: exploiting weaknesses in Russia's large military structure, carrying out precise attacks with limited but effective resources, and rapidly adapting to battlefield changes.

Precision strikes carried out by drones, whether kamikaze or reconnaissance types, have become Ukraine's primary tool for targeting ammunition depots, radar systems, command centers, and even military bases deep within Russian territory. This strategy damages the opponent's military infrastructure, creates psychological effects, and undermines Russian public confidence in their own national defense capabilities. Thus, Ukraine is not merely fighting with physical force but with tactical ingenuity and mastery of low-cost, flexible technology. This makes the Russia–Ukraine conflict a highly relevant contemporary case study for understanding the dynamics of modern asymmetric warfare. Drone technology, or unmanned aerial vehicles (UAVs), has become a symbol of transformation in modern warfare. Its ability to reach target areas without direct combat personnel involvement, combined with operational flexibility, makes drones an efficient, affordable, and lethal strategic instrument. On the Ukrainian battlefield, the use of drones has intensified and grown in complexity. Ukraine has not only deployed Western-made drones such as Turkey's Bayraktar TB2 but has also developed domestic drones and modified commercial drones into highly destructive improvised weapons.

Over time, Ukraine began integrating First-Person View (FPV) drones into its tactical strike strategy. FPV drones are typically small camera-based drones controlled in real-time from the pilot's perspective, similar to systems used in civilian drone racing. However, in military versions, FPV drones are equipped with explosives and manually guided to targets at high speed and with great precision. Their production cost is very low, ranging from USD 300–500 per unit, yet their effectiveness in destroying armored vehicles, defensive trenches, and even field command posts is significant. One of the main advantages of FPV drones is their high speed, small size, and ability to maneuver through obstacles and passive defenses. Russian radar and automated detection systems have struggled to detect and respond to such attacks, as their small size does not reflect on radar like larger aerial vehicles. According to a 2023 report by the Royal United Services Institute (RUSI), Ukrainian FPV drones have become one of the most disruptive weapons, damaging Russian combat vehicles more effectively than landmines or traditional anti-tank weapons.

More striking is the asymmetric nature of these drones' use. With production costs far lower than missiles or fighter jets, Ukraine can launch attacks that inflict substantial losses on the enemy without expending large-scale resources. This demonstrates how lightweight technology can create new imbalances on the battlefield and become a strategic tool to counter military dominance. This phenomenon affects not only the tactical dimension of war but also shakes the foundations of traditional military thought. Conventional air defense and intelligence systems have proven not always adaptive to new threats such as small, low-flying, autonomous drones. Thus, Ukraine's use of drones, including FPV variants, reflects not only military innovation but also signals a fundamental shift in how war is understood and conducted in the 21st century.

A key pillar of modern military structure is an intelligence system capable of providing early warnings of strategic threats. Intelligence functions include early detection, threat mapping, analysis of enemy intentions, and formulating anticipatory strategies. In conventional armed conflicts, the success of military operations heavily depends on the accuracy and speed of information gathered by intelligence agencies.

However, in the Russia–Ukraine war, Russia's intelligence system has failed glaringly to recognize and respond to drones as Ukraine's primary strike tactic.

Since mid-2022, Ukraine has consistently launched drone attacks on various strategic Russian targets, including those located far from the front lines. The attack on Engels Air Base in Saratov (December 2022), one of Russia's strategic bomber launch bases, demonstrated that strikes could reach deep into Russian domestic airspace undetected. This was not an isolated incident. Various logistical facilities, ammunition depots, and even energy infrastructure in Russia's border regions and major cities have suffered damage from Ukrainian drone attacks. Reports from the Institute for the Study of War (ISW) and the RAND Corporation indicate that Russia's radar systems and defense networks have failed to adapt to the new threat posed by high-speed, small drones like FPVs. Furthermore, the inability to predict strike points reflects poor coordination between Russian intelligence analysis, air defense forces, and early warning systems. Not only did intelligence fail to prevent attacks, but it also seemed incapable of formulating an effective response to Ukraine's evolving tactics on the ground.

Moreover, this failure is structural. The 2023 RUSI report mentions that Russia's rigid military bureaucracy, fragmented information flow, and top-down reporting culture have hampered the system's ability to adapt intelligence approaches to dynamic warfare. Consequently, innovations by adversaries, such as Ukraine's drone use, were not perceived as urgent threats until actual attacks repeatedly occurred. Russia's intelligence failure illustrates how asymmetric warfare weakens an opponent's physical power and exposes conceptual weaknesses in traditional military organizations. In wars increasingly dependent on rapid adaptation and artificial intelligence, slow, conventional, and hierarchical intelligence approaches can become vulnerabilities systematically exploited by the enemy.

Although the Russia–Ukraine conflict has been a central focus of international media and defense policy studies since 2022, much of the prevailing narrative remains descriptive. It focuses on the general operational aspects of the war. Academic studies specifically analyzing the dynamics of asymmetric warfare through drone use and its link to intelligence failures are still relatively limited, especially in the context of Russia as a major military power with a defense system long regarded as modern. Reports from strategic research institutions such as the RAND Corporation, RUSI, and CSIS have highlighted the effectiveness of drone tactics and the new challenges they pose to air defense. However, these reports mostly emphasize technical and operational aspects, not a systemic analysis linking drone-based asymmetric strategies with fundamental vulnerabilities in a superpower's intelligence architecture. This indicates significant room for the development of academic discourse that discusses weapons as technological entities and as symbols of fundamental changes in the character of conflict and how major powers structure their defense posture.

This study, therefore, seeks to fill this gap by examining how Ukraine's drone attacks systematically exploit Russia's intelligence weaknesses and represent a new form of asymmetric warfare that is no longer based on troop numbers or heavy weaponry but on speed of adaptation, tactical improvisation, and the use of low-cost yet precise technology. The urgency of this study is heightened by the fact that the conflict in Ukraine is not merely a military clash between two countries but also reflects the future direction of warfare. For other countries, especially those with limited military resources, similar strategies could become viable alternatives for building deterrence against external threats. Conversely, for major powers, this study may provide critical input for reassessing their intelligence and defense structures to become more responsive to new, unconventional threat forms. Therefore, this research is theoretically relevant within the security and military studies field and holds practical value for formulating defense policies and reforming intelligence systems at national and global levels.

2. Literature Review

2.1. Asymmetric Warfare

Asymmetric warfare describes a form of conflict that occurs between two parties with a significant imbalance of power. This disparity may manifest in various aspects such as technology, strategy, resources, and even the objectives sought. This phenomenon has become increasingly relevant in modern warfare, especially when non-state actors or states with limited military capacity confront far more dominant conventional military powers.

According to Mello (2016), asymmetric warfare is a type of combat in which the opposing sides' goals, methods, and means differ significantly. Such conflicts often involve states fighting non-state actors using unconventional methods such as guerrilla warfare or terrorism. Barisić and Vračar (2023) state that asymmetric warfare entails complex strategic relationships between unequal parties. Unlike guerrilla warfare or insurgencies alone, this concept accounts for the strengths and weaknesses of each actor involved.

Ancker and Burke (2003) argue that asymmetric warfare requires a flexible and adaptive military doctrine. This is due to the high uncertainty encountered when confronting an unconventional adversary. A lack of preparedness in countering the opponent's tactical advantages frequently results in strategic failure. Caforio (2009) notes that asymmetric warfare has transformed the paradigm of modern militaries. It demands structural and mental transformation within the armed forces, requiring them to think beyond the frameworks of conventional military strategy. This type of warfare hinges not just on physical strength but also on adaptability in facing unpredictable situations.

Furthermore, Eaton (2002) emphasizes that although asymmetric warfare has existed since ancient times—as reflected in the biblical story of David and Goliath—it only gained prominence in modern military doctrine from the mid-1990s, when threats from non-state actors increased significantly. This change marked a turning point in strategic thought, compelling conventional forces to adapt to more unpredictable methods of warfare. Bolgár and Krajnc (2010) add that the psychological aspect of asymmetric warfare is crucial. Weaker actors often employ fear, surprise, and uncertainty to disrupt stronger opponents. This creates deep psychological tension and often makes the stronger side feel threatened despite having clear physical superiority.

Meanwhile, Angeren and Baan (2007) stress that success in asymmetric warfare does not depend on direct military victory. Instead, the key is enduring and continuously disrupting the adversary. For weaker groups, the primary goal is to sustain existence rather than achieve victory in the traditional sense. Asymmetric warfare challenges conventional views of conflict and changes how we understand unequal power dynamics. In a constantly evolving world where non-conventional power increasingly matters, asymmetric warfare has become an inevitable element in modern geopolitical dynamics.

2.2. Intelligence Failures

Intelligence failure is one of the critical factors that can lead to strategic losses in military operations. In a modern battlefield that is increasingly unconventional and rapidly changing, a lack of accurate information can significantly affect the outcome of a conflict. Such failures often stem from systemic and operational factors that can be difficult to avoid.

According to Bush (2001), military intelligence failures are often inevitable due to resource limitations, institutional biases, and errors in assessing the enemy's intentions and capabilities. In many cases, these factors lead to flawed conclusions and inadequate planning. Evans (2009) adds that intelligence failures frequently originate from internal dynamics within the military structure, such as overreliance on "received opinion", overconfidence, and a lack of integration between command and intelligence units.

Trafton (1994) emphasizes that one way to prevent such failures is by strengthening the functional link between operations and intelligence (OPS-INTEL). Enhanced coordination and cross-level training within the military structure are vital to ensure that intelligence supports operations efficiently and promptly. Azotea (2014) reminds us of the Korean War's failures, largely due to poor training and a shortage of well-trained intelligence personnel. Additionally, cultural biases in assessing threats from North Korea and China contributed to fatal errors in strategic analysis. On the other hand, Dahlin (2009) argues that a major cause of intelligence failures is military commanders' lack of understanding of potential errors within the intelligence process. Better communication and deeper awareness of intelligence decision-making processes are crucial to prevent similar failures.

In his analysis, Kahana (2005) reveals that Israeli intelligence faced many strategic and operational failures, such as during the Yom Kippur War, demonstrating weak early-warning capabilities due to organizational biases and incorrect assumptions about the enemy. A similar failure is seen in the 9/11 attacks, which, according to Ea (2017), show how bureaucratic structures and organizational reforms can

create vulnerabilities within the intelligence system. In these large, complex systems, failure becomes difficult to avoid, even with highly advanced structures.

2.3. Functions and Roles of Military Intelligence

Military intelligence is vital in supporting effective strategic, operational, and tactical decision-making in modern warfare. Its primary functions include collecting, analyzing, interpreting, and disseminating relevant information about the enemy's strength, intentions, and capabilities. This function is inseparable from every step taken by commanders in engaging the enemy.

According to Russell (2021), military intelligence is the art of "knowing the enemy," aiming to provide timely, relevant, and accurate information to commanders at all levels of military operations. Sadiku and Musa (2021) add that military intelligence draws on various disciplines, such as political theory, economics, psychology, and sociology, all of which guide military decision-making, especially in analyzing enemy strength and plans. Rietjens (2021) asserts that the function of intelligence in military missions is to help commanders understand the operational environment comprehensively. This process includes direction, data collection, analysis, and the dissemination of information to decision-makers, enabling them to respond swiftly and accurately. Additionally, Miller et al. (2004) identify seven main phases in the military intelligence process: planning, collection, processing, analysis, dissemination, mission evaluation, and communication—all designed to deliver an informational advantage on the battlefield.

According to Scheffler and Dietrich (2023), military intelligence also involves balancing intellectual independence with support for strategic decision-making. This is important to ensure that intelligence assessments remain consistent with objective national evaluations and are not influenced by political or organizational interests. Pecht and Tishler (2015) add that military intelligence is crucial in conventional warfare and in enhancing the effectiveness of weapons systems, preventing conflict through deterrence strategies, and supporting preemptive policies. In addressing the complexity of modern conflicts, Spoor and de Werd (2023) argue that military intelligence must be viewed as a highly situational practice. Intelligence now relies on informal collaboration and holistic approaches to respond to rapidly changing political and social dynamics and to anticipate threats that may arise from unexpected sources.

3. Methodology

This research uses a literature review method with a descriptive qualitative approach. The objective is to analyze the phenomenon of asymmetric warfare and Russia's intelligence failures in responding to Ukraine's drone attacks. Data are obtained from various secondary sources, such as scholarly journals, strategic think-tank reports, credible media publications, and open defense analyses. Literature is purposively selected based on thematic relevance, source credibility, and data recency, focusing on the 2014–2024. The analysis includes identifying main themes, classifying attack and response patterns, and interpreting findings based on asymmetric warfare theories and strategic intelligence. This method allows the author to construct data-driven, in-depth arguments without the limitations of direct battlefield observation.

4. Result and Discussion

4.1. Ukraine's Drone Attacks on Russian Military Infrastructure

Since the onset of Russia's invasion of Ukraine in February 2022, the Ukrainian military's use of unmanned aerial systems (drones) has evolved into a key strategy to counterbalance the conventional power disparity. Drones have been deployed for reconnaissance and modified to directly strike strategic targets with high cost-efficiency and significant operational impact. One of the first significant attacks occurred in December 2022, when Ukraine successfully struck Engels Air Base in Saratov, Russia. This base is one of the launch sites for Russia's Tu-95MS strategic bombers. The attack killed several military personnel and damaged aircraft as well as other critical infrastructure (Nagl & Crombe, 2024).

In the following years, the intensity and scale of these attacks continued to grow. A maritime drone strike on the Crimean Bridge (Kerch Bridge) in mid-2023 caused major disruptions to Russian military supply lines in the south, demonstrating Ukraine's capability to hit strategic assets from afar. In early May

2025, Ukraine launched another large-scale drone attack on multiple Russian military airbases, according to reports by BBC Indonesia and Kompas. One of the most notable strikes targeted airbases in Belgorod and Voronezh, which are used as launch points for Russian air operations against Ukraine.

According to an NTVNews (2025) report, the attack employed a mix of locally produced kamikaze and modified commercial drones. Some drones had AI-based smart navigation systems designed to evade Russian radar and Pantsir-S1 air defense systems. As a result, several hangars and fighter aircraft were reported destroyed, and flight operations in those areas were disrupted for over 24 hours. These attacks demonstrate two critical points: first, that Ukraine has significantly improved the technical sophistication of its drone systems; and second, that Russia's detection and air defense systems remain largely ineffective at countering large-scale drone attacks, even when the targeted areas are deep inside Russian territory.

According to Gioe (2018), many analysts highlight that Russia's intelligence apparatus still clings to a Cold War–era approach, relying heavily on HUMINT, strategic signals, and hierarchical command structures. This approach lacks the flexibility needed to handle the fast-paced dynamics of modern drone warfare. Shrivastava (2018) similarly notes that Russia's dependence on conventional strength was evident in its slow response to small-scale UAV attacks on the Khmeimim airbase in Syria in 2018. This attack caught Russian defenses by surprise and exposed their unpreparedness for asymmetric drone tactics.

Russia's inability to anticipate Ukraine's drone attacks reflects not only technical defense weaknesses but also dysfunction within its military intelligence system. Russia was expected to detect and prevent medium- to large-scale attacks as a major military power with a global intelligence network. However, empirical evidence shows that Ukrainian strikes — even those reaching as far as Moscow and Saratov — have repeatedly taken Russian forces by surprise and caused significant damage.

Russia's intelligence structure, which depends on HUMINT and SIGINT, is better suited for large-scale conflicts or long-term infiltration rather than detecting low-signature, rapid drone operations. This has resulted in failures to predict and intercept Ukraine's fluid, modular drone missions. By contrast, Bender & Staggs (2023) report that Ukraine has excelled in intelligence adaptation through open-source intelligence (OSINT), commercial technology, and a more decentralized, faster decision-making structure. OSINT allows Ukraine to track and respond to Russian troop movements flexibly and in near real-time. Civilian participation and open-source software further enable Ukraine to detect drones cheaply and effectively — an approach incompatible with Russia's rigid top-down command system. According to the BBC (2025), Russian defense authorities have often denied or delayed acknowledging drone attacks, indicating that internal intelligence reporting processes are neither prompt nor transparent. This has resulted in sluggish responses to emerging threats, particularly repeat attacks on military bases such as Engels, Dyagilevo, and Voronezh.

Some analysts, including Kurt Volker in his article for the Center for European Policy Analysis (CEPA), argue that Russia's primary intelligence failure lies in underestimating Ukraine's capacity for technological improvisation. Russia's intelligence focus remains conventional and doctrinal, leaving it unprepared for an asymmetric warfare model that repurposes civilian technology (like commercial drones) as offensive weapons. Moreover, Russian intelligence has appeared unable to map Ukraine's decentralized UAV production and distribution networks. Ukraine relies not only on Western-supplied drones but also on domestic manufacturing and open-source modification techniques spread through local drone communities. This lack of anticipation has repeatedly left Russia overwhelmed by low-cost yet high-impact drone strikes.

The series of successful Ukrainian drone attacks on Russia's strategic military facilities highlights structural unpreparedness and functional paralysis within Russia's intelligence apparatus. Despite having one of the world's largest and most experienced military intelligence networks, Russia has visibly failed to detect asymmetric, non-conventional threats. This failure primarily stems from the inability of its early-warning systems to identify threats posed by lightweight drone technologies, even when targets are highly secured military hubs.

A clear example of this paralysis can be seen in the strikes on Engels and Dyagilevo Air Bases at the end of 2022. Both facilities play strategic roles in Russia's air operations, but were successfully attacked by Ukraine's long-range drones without any early warning. Furthermore, Russia's air defense systems — which should benefit from robust intelligence — failed to intercept drones that penetrated hundreds of

kilometers behind the front lines. This indicates that Russia's radar sensors and signal-based or remote-sensing intelligence equipment lack the accuracy and operational scope needed to counter Ukraine's modular, low-observable drone tactics.

The delayed reaction of Russian authorities following these attacks further reinforces suspicions that reporting and coordination among intelligence agencies, air defenses, and public media are not functioning synchronously. In multiple incidents, Russian authorities confirmed attacks only hours or even days after they occurred — and in many cases, no statement was given at all. Such slow and opaque responses reveal structural disorientation and possible information distortion within Russia's military hierarchy. The recurring nature of these drone attacks — with similar patterns — suggests that Russia has not implemented a sufficiently responsive strategic learning process. Even though Ukraine's drone infiltration techniques and routes are widely known to international observers, strikes continue to happen with high effectiveness. Russia's inability to disrupt Ukraine's drone supply chain or destroy launch infrastructure behind enemy lines further supports the impression that Russian intelligence has failed to detect and undermine the opponent's preparations proactively. In modern warfare — where intelligence is not just a passive surveillance tool but a core component of preventive action — this condition amounts to a serious and systemic paralysis.

Russia's intelligence failure in countering Ukraine's drone strikes has implications that go beyond technical and tactical aspects; it affects the strategic balance in the region and global perceptions of Russian military power. Internationally, Ukraine's ability to carry out precise strikes deep inside Russian territory using relatively cheap weapons has shifted paradigms regarding what constitutes military superiority. Russia, long perceived as having formidable air defense and intelligence networks, now finds itself symbolically and operationally exposed by a conventionally weaker adversary. This situation also undermines Russia's military credibility in the eyes of both the international and domestic public. When Ukrainian drones reach areas near Moscow or hit strategic structures like the Kerch Bridge with minimal resistance, the message is not just about Ukraine's tactical success but also about Russia's failure to secure its own airspace. Consequently, public trust in Russia's security and military leadership tends to decline, and the legitimacy of its military policies erodes further.

Additionally, Russia's dependence on conventional defense structures limits its flexibility in adapting doctrine to new threats. Its reluctance to adjust its approach to nonlinear forms of warfare has only exacerbated existing weaknesses. Rather than responding with technological and tactical innovation, Russia appears more inclined to control the public narrative through propaganda, censorship, and nationalist rhetoric — actions that distance it further from the battlefield's objective reality. This gap between perception and reality risks diminishing military preparedness in the long term. Another critical implication is that Ukraine's asymmetric strategy sets a precedent for other smaller states, showing that deterrence against major powers can now be achieved without possessing ballistic missiles or expensive weapons systems. Drone warfare has demonstrated that military advantage is no longer solely about quantity and size of armaments but about speed of adaptation, technological creativity, and tactical ingenuity. This marks the emergence of a new phase in the evolution of warfare, redefining the concept of military power in the 21st century.

4.2. Intelligence Dysfunction in Drone Warfare

The evolution of modern warfare shows that intelligence effectiveness is no longer determined merely by data collection capacity, but by an institution's ability to adapt to the changing nature of threats. In this regard, Russian intelligence has faced significant challenges when confronting Ukraine's drone warfare strategy. Instead of being able to anticipate and respond adaptively, Russia's intelligence system has demonstrated dysfunction in interpreting the new patterns of asymmetric warfare, especially those characterized by lightweight, highly disruptive technology.

Historically, Russian intelligence developed from a highly hierarchical model focused on conventional, physically measurable threats such as troop concentrations, logistics, and heavy weapon systems. This approach has produced an information-processing system that is slow, bureaucratic, and heavily reliant on centralized decision-making mechanisms. When Ukraine began using drones to strike strategic Russian sites—such as Engels Air Base and military facilities in Voronezh and Belgorod—these attack patterns failed to be detected or preempted. This reveals a fundamental mismatch between the design of Russia's intelligence system and the nature of the threats it now faces.

Ukraine's aerial strikes no longer require large fleets or complex flight routes. Instead, modified low-cost drones launched from concealed locations and controlled with autonomous navigation systems have enabled Ukraine to penetrate deep into Russian territory undetected by radar. Here, the structural weakness of Russian intelligence becomes evident. Surveillance instruments such as the S-400 radar or Pantsir-S1 systems, which are designed to counter large-scale air raids, have proven ineffective against small, fast-moving tactical drones. A report by the Center for European Policy Analysis (CEPA) in 2024 highlighted that Russia's intelligence system is too slow to respond to attacks requiring rapid, on-the-ground decision-making. When Russian military authorities must wait for central command verification before taking action, a drone attack lasting only a few minutes will already have caused damage. This weakness is exacerbated by the absence of a dedicated unit within Russia's military structure to monitor drone threats in real-time—something Ukraine has addressed through a combined military, civilian, and semi-independent drone community intelligence network. In contrast, Ukraine leverages resource flexibility and an open-source technological approach, making it more adaptive and innovative. Information gathered via commercial satellites, small reconnaissance drones, and civilian reports is mobilized into a decentralized attack strategy. Here lies the stark difference between two intelligence models: Russia's centralized, closed, and slow system versus Ukraine's rapid, collaborative, and responsive model suited for a dynamic battlefield.

Therefore, Russia's intelligence system dysfunction is not merely technical or incidental. Rather, it is symptomatic of an institutional structure unprepared for an era of unconventional, technology-driven warfare. The inability to read the changing battlefield signs leaves Russia more vulnerable to attacks executed with speed, surprise, and minimal disruption.

4.3. Weaknesses in Early Detection and Threat Analysis

One of the clearest indicators of Russia's intelligence failure in countering Ukraine's drone strategy is its weak capacity for early threat detection. In modern warfare, early warning is not simply a technical matter but the foundation of a defense system that enables rapid action to prevent or mitigate attack impacts. When Ukrainian drones repeatedly reach strategic targets within Russian airspace unimpeded, it is clear that Russia's early warning and threat analysis systems are not functioning optimally. According to Humennyi et al. (2024), despite Russia possessing extensive radar and early-warning satellite networks, various long-range drone strikes by Ukraine—including those on Engels and Dyagilevo—have successfully hit strategic targets without interception, indicating that these systems cannot detect low-profile objects like small or kamikaze drones.

Technologically, Russia is known to have one of the most advanced air defense networks in the world, including the S-400, Pantsir-S1, and long-range radars. However, these systems are limited in effectiveness against drones with small radar cross-sections, low speeds, and unconventional routes. The drones Ukraine uses—often locally modified or commercially sourced—are designed to avoid detection by military radars typically programmed to track fighter jets or ballistic missiles. Consequently, despite having sophisticated hardware, Russia's detection systems appear poorly adapted to identify and track small, unpredictable drones, which are a hallmark of modern drone attacks.

Furthermore, this weakness is technical and reflects a shortfall in intelligence information processing. Data gathered from sensors, satellite imagery, or signal communications often fails to translate quickly into actionable field warnings. According to a 2024 report by the Institute for the Study of War (ISW), in many cases, Russian military commands only learned of attacks after physical damage occurred or after visual reports appeared on social media and from civilians. This demonstrates that available information was not mobilized effectively for rapid decision-making. In drone warfare, where speed and surprise are critical, even a few minutes' delay can determine whether an attack is thwarted or succeeds.

The December 2022 attack on Engels Air Base is a key example of this failure. Although the base is located hundreds of kilometers from the Ukrainian border, a strike drone managed to penetrate defenses and hit ammunition storage and strategic aircraft. There was no significant interception or prevention record, and Russia issued a public statement only hours after the incident. Similar scenarios repeated with attacks on Dyagilevo, Voronezh, and Belgorod throughout 2023 and 2024. The absence of an effective early warning system indicates that the risk of such attacks was not prioritized or ignored in threat assessments. According to Kim & Cho (2023), this supports evidence that Russia's detection system is incapable of real-

time drone tracking, especially when launches occur from unexpected locations and with unconventional flight paths.

This systemic weakness is compounded by the military bureaucracy's failure to conduct accurate threat modeling. Drones are not considered a major strategic threat but merely a tactical nuisance. This narrow perspective has slowed Russia's development of appropriate defensive capabilities, both technologically and regarding human resources. As a result, although information about Ukraine's increased drone production and use was available through open sources, no meaningful mitigation steps were taken to strengthen early detection, whether through micro-radar development or the establishment of rapid-response drone-hunting units. Thus, the shortcomings in early detection and threat analysis are not just about technical limitations but are a manifestation of structural failure rooted in flawed intelligence assumptions and priorities. In a battlefield increasingly dominated by autonomous systems and non-conventional strategies, failing to adapt detection methods and analytical models becomes a critical factor driving strategic vulnerability.

4.4. Failure to Anticipate Ukraine's Asymmetric Strategy

Russia's intelligence ineffectiveness in countering Ukraine's drone attacks is not only about technical failures and poor early detection but also about structural incapacity to understand and anticipate shifts in the opponent's warfare strategy. Ukraine's asymmetric strategy since 2022 reflects an approach markedly different from conventional warfare: rather than attempting to capture territory directly, Ukraine aims to cripple the enemy's combat capability through sustained pressure on strategic nodes using limited yet effective resources. Here, Russian intelligence has shown little capacity to read the direction and strategic objectives behind Ukraine's actions. Drone strikes targeting airbases, ammunition depots, fuel supply chains, and military logistics networks signal a shift from traditional military strategy to systemic disruption. Rather than open confrontation, Ukraine has chosen to exploit the enemy's blind spots and weak points with precision and control. According to Gady & Kofman (2023), Ukraine systematically uses drones not only for reconnaissance but as primary tools in a modern form of attrition warfare, gradually draining Russian resources through sustained, low-cost drone attacks on military infrastructure.

Intelligence agencies should have read this attack pattern as part of a modern attrition warfare approach, where gradual depletion is achieved through repeated cheap technological pressure. Yet, by 2025, there is no evidence that Russia has developed a comprehensive strategic map to respond to or preempt this approach. According to Chavez & Swed (2023), Russia has repeatedly underestimated Ukraine's speed and capacity to modify commercial drones into dangerous weapons. Ukraine has innovatively leveraged cheap, market-available drones and converted them into effective combat tools at scale. One sign of this unpreparedness is Russia's low investment in developing defense systems designed to counter low-cost, commercially based drones. Despite Ukraine openly ramping up local drone production and adopting drone swarming tactics since early 2023—launching dozens of small drones simultaneously to overwhelm enemy defenses—Russia has persisted with conventional air defense systems and front-line military posturing without crafting targeted solutions for unmanned aerial threats.

Consistent with Kunertova's (2023) findings, Russia's response to Ukraine's drone innovations has been defensive, reactive, and technologically and doctrinally inflexible. Russia remains heavily reliant on conventional air defense systems not designed to counter small, low-signature drones and has been slow to develop counter-drone capabilities. Moreover, Ukraine's success in modifying civilian drones into tactical weapons adds complexity to this conflict. Commercial drones like the DJI Mavic, outfitted with explosives or surveillance cameras, illustrate how flexibility and improvisation are key advantages in asymmetric warfare. This strategy demonstrates that technological strength is not determined by the sophistication of instruments alone but by adaptability and integration with battlefield realities. While Ukraine continues to exploit open-source resources and civilian technology, Russia remains stuck in a closed military technology paradigm that cannot react swiftly and efficiently. Russia's intelligence failure to anticipate such scenarios stems not only from hardware limitations but also from a conceptual gap in understanding the changing dynamics of warfare.

The inability to read and map the opponent's non-linear strategy is also evident in Russia's sporadic and reactive responses. Drone attacks are often countered by adding artillery or missile defense units, rather than through systemic approaches involving enhanced prediction capacity, battlefield intelligence modernization, or strengthened small-tech combat units. By contrast, Ukraine has created autonomous

drone units within its military structure, granted local operational authority, and employed AI for rapid field decision-making. This contrast highlights the adaptive gap between the two sides.

In summary, Russia's intelligence failure is not simply a failure to detect attacks but a deeper failure to interpret a new strategic map deployed by a smaller, more flexible, and more adaptive adversary. A rigid, centralized, and sluggish intelligence model becomes vulnerable and irrelevant as warfare moves toward networks, decentralization, and speed. Russia's inability to align with the asymmetric characteristics of Ukraine's approach is a fundamental weakness that its adversary has exploited to maximize effect.

4.5. Intelligence Failure as a Systemic Symptom

Russia's intelligence failure in responding to Ukraine's drone attacks cannot be viewed merely as the result of technical oversights or operational mishaps. Instead, this failure manifests deeply rooted systemic weaknesses within the structure and institutional culture of Russia's defense and security apparatus. The repeated pattern—delayed detection, flawed analysis, and disproportionate responses—makes clear that the problem is not confined to functional units but represents a broader institutional crisis.

One of the most evident systemic symptoms is extreme decision-making centralization within Russia's military and intelligence structures. According to Dylan et al. (2024), Russia's intelligence failure to anticipate Ukraine's 2022 invasion was not merely operational but reflected systemic stagnation within a highly hierarchical, non-transparent national security framework. This structure creates inefficient information flow and hampers data-driven decision-making. Riehle (2024) similarly points out that Russian intelligence has focused more on maintaining narratives of success domestically than acknowledging and learning from strategic mistakes, especially in the early stages of the war. This widens the dissonance between battlefield reality and official reports submitted to top leadership. In such a rigid system, strategic decision-making and threat responses often wait for top-level directives, which slows reaction time to rapidly unfolding situations. In the case of drone attacks, where strikes can occur and conclude in mere minutes, such rigid decision mechanisms are highly ineffective. This contrasts with Ukraine's more decentralized model, where local units are granted full authority to act based on real-time conditions.

Moreover, Russian intelligence's organizational culture is often repressive toward failure and internal correction. A Royal United Services Institute (RUSI) report notes that Russian military and intelligence personnel tend to be reluctant to deliver reports that conflict with the success narratives expected by leadership. As a result, field information indicating weaknesses or new threats is often filtered or even concealed, causing strategic decisions based on distorted information. This creates a policy loop unresponsive to operational realities, even when threats are clear and recurring.

This systemic crisis is exacerbated by minimal cross-agency integration, especially among key bodies like the FSB, GRU, and Ministry of Defense. Weak institutional coordination means information gathered by one agency is not fully utilized by another. For example, military satellite reconnaissance data is not always linked to air defense rapid warning systems, resulting in lost opportunities to intercept attacks amid lengthy and inefficient bureaucratic processes. This lack of interoperability further worsens Russia's inability to respond to drone threats in a comprehensive and coordinated manner.

Additionally, Russia's large military modernization budget has largely been allocated to reinforcing conventional assets such as submarines, fighter jets, and hypersonic missiles. Meanwhile, the need to modernize intelligence and develop defenses against new threats—like autonomous drones and AI-enabled electronic warfare systems—has been neglected. This imbalance reflects a strategic perspective still rooted in a 20th-century warfare paradigm rather than the distributed technology and information-driven warfare of the 21st century. This systemic failure creates operational vulnerabilities and risks fracturing institutional legitimacy over time. When military units continue to suffer repeated attacks without adequate protection, while success narratives are forcibly maintained at the top, discord emerges between frontline experience and central perception. This undermines internal trust, lowers troop morale, and ultimately diminishes the overall effectiveness of the military structure.

Therefore, Russia's intelligence failure in responding to Ukraine's drone threat is not simply a technical issue or tactical oversight but a reflection of systemic shortcomings spanning structural, cultural, and

leadership dimensions. Without fundamental reforms, this system will repeat its failures when confronted with increasingly complex and unpredictable forms of modern warfare.

5. Conclusion

The drone attacks launched by Ukraine against various strategic Russian military infrastructures illustrate the transformation of modern warfare, which challenges conventional superiority through non-linear tactics and affordable yet highly effective technology. This phenomenon underscores the defining characteristics of asymmetric warfare, in which an actor with limited military capabilities can disrupt and even incapacitate a stronger adversary through technological innovation and flexible strike strategies.

Russia's failure to detect, prevent, and respond effectively to these unmanned aerial attacks reveals the weaknesses within its intelligence system, particularly when facing threats that do not fit traditional conflict patterns. Several successful strikes that reached sensitive facilities in supposedly well-protected areas—such as the attacks on Engels Air Base and ammunition depots in Belgorod—highlight deficiencies in early warning systems and the limitations of predictive analysis in anticipating unconventional forms of attack. Analysis of various literature and open-source reports, including findings from the Institute for the Study of War (ISW), RAND Corporation, and Western intelligence assessments, indicates that Russia faces serious challenges in adapting its command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems. This is further exacerbated by bureaucratization within its defense system and fragmentation between operational and intelligence units, resulting in slow and inaccurate responses to rapidly evolving threats.

On the Ukrainian side, the effective use of drones—whether modified commercial models or military-grade UAVs such as the Bayraktar TB2 and UJ-22 Airborne—reflects a strategy based on agility, mastery of the digital battlefield, and the deployment of a collaborative, real-time intelligence network. This approach has provided significant advantages, particularly in creating psychological effects, lowering enemy troop morale, and disrupting the opponent's logistical supply chains.

Based on these findings, it can be concluded that technological military superiority alone does not guarantee effective defense without an intelligence capability that is adaptive, integrated, and grounded in a deep understanding of emerging threat patterns. Low-tech asymmetric warfare, such as drone-based operations, demands a reformed intelligence system more responsive to fluid threats that cannot be mapped statically. This conflict offers an important lesson: that contemporary military resilience depends on the strength of heavy weaponry and the ability to read subtle signs, anticipate new attack patterns, and respond rapidly and accurately.

References

Ancker, C., & Burke, M. (2003). Doctrine for Asymmetric Warfare. *Military review, 83*, 18.

Angeren, J., & Baan, A. (2007). Game theory and asymmetric warfare - is there a match?

Azotea, C. (2014). Operational Intelligence Failures of the Korean War.

Barišić, I., & Vračar, M. (2023). Theoretical starting points in considering the concept of asymmetric warfare. *Vojno delo*. https://doi.org/10.5937/vojdelo2304022b.

Bender, C., & Staggs, J. (2023). Leveling the Playing Field: Equipping Ukrainian Freedom Fighters with Low-Cost Drone Detection Capabilities. *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, 287-312. https://doi.org/10.23919/CyCon58705.2023.10181421.

Bolgár, J., & Krajnc, Z. (2010). Some thoughts about psychological questions of asymmetric warfare.

Bush, B. (2001). The Logic of Military Intelligence Failures. https://doi.org/10.21236/ada401287.

Caforio, G. (2009). Asymmetric warfare: an introduction. https://doi.org/10.1108/S1572-8323(2009)000012A019.

Chávez, K., & Swed, O. (2023). Emulating underdogs: Tactical drones in the Russia-Ukraine war. *Contemporary Security Policy, 44*, 592 - 605. https://doi.org/10.1080/13523260.2023.2257964.

Commander, W., & Eaton, J. (2002). The beauty of asymmetry: An examination of the context and practice of asymmetric and unconventional warfare from a western/centrist perspective. *Defence Studies, 2*, 51 - 82. https://doi.org/10.1080/14702430208405011.

Dahlin, R. (2009). Intelligence Failure: How a Commander Can Prevent It.

Ea, Y. (2017). The Enemy Achieves Surprise: Are Intelligence Failures Avoidable?. *Journal of Political Sciences & Public Affairs, 5*, 1-5. https://doi.org/10.4172/2332-0761.1000311.

Evans, G. (2009). Rethinking Military Intelligence Failure – Putting the Wheels Back on the Intelligence Cycle. *Defence Studies, 9*, 22 - 46. https://doi.org/10.1080/14702430701811987.

Gady, F., & Kofman, M. (2023). Ukraine's Strategy of Attrition. *Survival, 65*, 7 - 22. https://doi.org/10.1080/00396338.2023.2193092.

Gioe, D. (2018). Cyber operations and useful fools: the approach of Russian hybrid intelligence. *Intelligence and National Security, 33*, 954 - 973. https://doi.org/10.1080/02684527.2018.1479345.

Institute for the Study of War (ISW). (2024–2025). Russia Campaign Assessments. https://www.understandingwar.org.

Kahana, E. (2005). Analyzing Israel's Intelligence Failures. *International Journal of Intelligence and CounterIntelligence, 18*, 262 - 279. https://doi.org/10.1080/08850600590882146.

Mello, P. (2016). Asymmetric Warfare. https://doi.org/10.1002/9781405165518.wbeos0773.

Miller, J., Pawling, C., & Chambal, S. (2004). Modeling the U.S. Military Intelligence Process.

Nagl, J. A., & Crombe, K. (2024). A Call to Action: Lessons from Ukraine for the Future Force. *U.S. Army War College Press*.

Pecht, E., & Tishler, A. (2015). The value of military intelligence. *Defence and Peace Economics, 26*, 179 - 211. https://doi.org/10.1080/10242694.2014.886435.

Rietjens, S. (2021). Intelligence in Military Missions: Between Theory and Practice. *Handbook of Military Sciences*. https://doi.org/10.1007/978-3-030-02866-4_96-1.

Russell, F. (2021). Military Intelligence. *A Companion to Greek Warfare*. https://doi.org/10.1002/9781119438847.ch19.

Sadiku, M., & Musa, S. (2021). Military Intelligence. *A Primer on Multiple Intelligences*. https://doi.org/10.1007/978-3-030-77584-1_20.

Scheffler, A., & Dietrich, J. (2023). Military Intelligence: Ill-Defined and Understudied. *International Journal of Intelligence and CounterIntelligence, 36*, 1047 - 1066. https://doi.org/10.1080/08850607.2023.2187190.

Shrivastava, A. (2018). mAss AttAck by DroNes: FAciNg the chAlleNge.

Spoor, B., & De Werd, P. (2023). Complexity in Military Intelligence. *International Journal of Intelligence and CounterIntelligence, 36*, 1122 - 1142. https://doi.org/10.1080/08850607.2023.2209493.

Trafton, D. (1994). Intelligence Failure and Its Prevention. https://doi.org/10.21236/ada279514.

https://www.ntvnews.id/news/0149943/serangan-drone-ukraina-guncang-pangkalan-udara-rusia.

https://video.kompas.com/watch/1851739/ukraina-melancarkan-serangan-drone-besar-besaran-ke-pangkalan-udara-rusia-jelang-perundingan-damai

https://www.bbc.com/indonesia/articles/c9dq4le3n43o