OPERATING ENVIRONMENT

Strategic Analysis of the Russia–Ukraine War and Implications for Euro-Atlantic Security

2023 - 2025

Zdenek PETRAS

University of Defence of Defence
Centre for Security and Military Strategic Studies | Brno 2026

Author:

Zdenek PETRAS, PhD. (Colonel ret.) graduated from the Military College of Land Forces in Vyskov (CZE). In 2008, he completed a master´s degree at the Université Panthéon-Assas Paris II, in defence industry dynamics. In 2016, he obtained a PhD. degree in economics and management program at the University of Defence Brno (CZE), specialising in military capability assessment. After several years as a staff officer at the General Staff of the Czech Forces and in NATO and EU military structures, he currently works as a research fellow at the Centre for Security and Military Strategic Studies. He is systematically engaged in issues related to military strategy, defence planning and capability development. He is the author of several articles and publications on these topics.

University of Defence

Centre for Security and Military Strategic Studies

The Centre for Security and Military Strategic Studies is part of the University of Defence and is defined as another workplace for education and creative activity pursuant to the Act No. 111/1998 Coll., Section 22, Paragraph 1, Letter c). Its mission is in particular:

- Scientific and research activities in the areas of security studies, strategic leadership, military art, strategic management and defence planning, implemented for the needs of the strategic level of decision-making, state defence management and building the Armed Forces of the Czech Republic;
- Training of military and civilian experts of the Ministry of Defence and the Armed Forces in professional and career courses (General Staff Course, Senior Officers Course);
- Professional, publishing and popularisation activities (including sponsorship of the Czech Military Review and Defence and Strategy magazines).

The analytical study is the result of research conducted by the Centre for Security and Military-Strategic Studies and is supported by the Ministry of Defence of the Czech Republic within the Program of Long-Term Development of Organisation – Armed Conflict (DZRO OZKON).

Reviewers:

COL. Jaroslav KOMPAN, PhD.

doc. Ing. Ivan MAJCHÚT, PhD.

Publisher: University of Defence Brno, Czech Republic

Year of Publication: 2026

ISBN 978-80-7582-688-6

ISBN 978-80-7582-689-3 (online; pdf)

Table of Contents:

FOREWORD

The Centre for Security and Military-Strategic Studies, through its research and expert activities, is preparing a study examining global geopolitical trends and the evolving operating environment—understood as the set of conditions that shape the nature and conduct of modern conflicts. The aim is to guide the transformation of armed forces, ensuring they can adapt effectively to this rapidly changing environment.

This analysis of the operational environment is inherently forward-looking: it provides a strategic-military assessment of the future to inform decisions that can shape it. By examining current and emerging trends, it seeks to support decision-making regarding the development of armed forces, enabling them to anticipate challenges, exploit opportunities, and maintain operational effectiveness in increasingly complex scenarios.

In the context of the ongoing conflict in Ukraine, the operational environment is demonstrating a rapid transformation of warfare, characterised by technological acceleration, the growing role of unmanned systems, and the centrality of information and cyber operations. These developments underscore that the coming years are likely to be marked by crises and conflicts involving actors pursuing strategic interests, with democratic armed forces continuing to play a decisive role in defending their nations, maintaining international peace and stability, and safeguarding the security and well-being of their citizens.

The primary objective of this document is to present ideas that anticipate the most significant potential future strategic events. By understanding these developments in advance, decision-makers can shape policies and investments today that will guide the development of future armed forces, ensuring their continuous adaptation to a new and uncertain operational environment.

Equally important, this study aims to raise public awareness of defence and security issues. By highlighting emerging challenges and threats that could affect national stability in the near future, it seeks to promote a proactive approach to national security—one that requires not only the preparedness of our armed forces but also active cooperation with international partners.

INTRODUCTION

In February 2026, the Russian full-scale military invasion is entering its fourth year, now in its most intense phase and the period of greatest international visibility. According to the Russian Armed Forces' initial intentions, the campaign was expected to be rapid and precise, conducted as a limited operation and, ideally, maintained at a low level of intensity. This is evidenced by the relatively limited force package employed at the outbreak of hostilities, the strong operational thrust directed towards key urban centres such as Kyiv, Odesa and Kharkiv, as well as by the assumption that Ukrainian society and the Armed Forces of Ukraine, assessed as inferior in manpower and equipment, would either be unwilling or unable to resist.

The objective of this blitzkrieg-style operation was to force the rapid capitulation of the government in Kyiv and replace it with an authority more closely aligned with Moscow's strategic interests and requirements. Ukrainian resistance, which during the initial months benefited only from relatively limited Western support, proved far more effective—in terms of adaptability, operational effectiveness and combat intensity—than anticipated by Russian planners, as well as by part of the analytical community and Western public opinion. Kyiv successfully disrupted Moscow’s initial operational design, denied Russian air superiority, recaptured part of the occupied territory, conducted offensive operations into Russian territory, and compelled Moscow to fight a protracted, costly, and high-intensity positional and attritional war.

The art of war is changing before our eyes, and Ukraine has become the most advanced laboratory for this transformation, while much of the world continues to prepare for conflicts rooted in the past. One of the most significant lessons emerging from the conflict that began in 2022 is the radical transformation of the soldier’s role. Human beings have become the most valuable, most vulnerable, and simultaneously the most difficult-to-replace resource on the battlefield, while numerous weapons systems that dominated military thinking at the turn of the 20th and 21st centuries are losing their central position. Tanks, heavy artillery, and traditional platforms are increasingly costly and ever less capable of surviving in a sensor-saturated environment of automated threats.

Unmanned systems of all types are taking their place. Within just a few years, these systems have become the core of a new military doctrine, fundamentally reshaping both the structure of armed forces and the very meaning of combat. Remotely operated platforms no longer require large crews; they are smaller, more agile, and easier to produce. Consequently, their overall combat power is growing exponentially, while unit costs are sharply declining and production is reaching industrial scale.

An increasing number of armed forces now operate drones, sensors, and automated systems, while units in more traditional roles focus on specific tasks such as special operations, reconnaissance, or logistics. The war in Ukraine has demonstrated that the modern battlefield is dominated by an extensive “kill zone,” up to forty kilometres deep along the entire front line. This zone is continuously monitored by drones capable of identifying and neutralising nearly any concentration of infantry or equipment.

In this context, operations are increasingly conducted by operators located far from the front line, hidden in rear areas or underground bunkers, while attempts at large-scale mechanised breakthroughs are largely doomed to fail. Instead of tank columns and artillery duels, modern offensives demand extreme dispersion of forces, concealment, and patience, with the objective of gradually advancing the pressure zone deep into the enemy's rear areas. Success depends on the ability to rapidly produce large quantities of inexpensive combat drones and continuously update their control systems. The initial phase of conflict, in which a single drone targeted a single objective, is becoming a thing of the past. Today, artificial intelligence allows a single operator to control entire fleets of drones simultaneously, monitoring kilometres of the front line rather than a few hundred meters.

These developments may create the misleading perception that future conflicts will reduce the need for mass mobilisation and place greater emphasis on the professionalism, technical readiness, and adaptability of individual operators. However, this assumption may prove deceptive. If a technologically advanced force confronts an unprepared adversary, the outcome may be rapid collapse under the intensity of modern warfare. When both sides are capable of adaptation, however, conflict is more likely to evolve into a prolonged positional and attritional struggle, in some respects reminiscent of the First World War. Under such conditions, operational success depends not only on technology but also on the ability to generate and sustain forces, maintain uninterrupted logistical flows, preserve combat effectiveness and morale, and control critical strike zones while simultaneously disrupting the adversary’s logistics, energy infrastructure, and communications through targeted attacks.

At the strategic level, the most important targets are no longer only soldiers in open terrain, but also weapons factories, logistics hubs, and command posts hidden in rear areas or underground. Their destruction requires long-range strike capabilities, forcing military planners to reassess reliance on expensive piloted aircraft and gradually replace them with reusable strategic drones. Tests of unmanned aircraft are already underway, paving the way for the widespread use of guided bombs—far cheaper than missiles—and the potential use of these drones as true “aircraft carriers” for swarms of kamikaze drones.

The same principles apply at sea, where Ukrainian naval drones have demonstrated the ability to inflict significant damage on units of the Russian Black Sea Fleet and even strike the so-called shadow fleet of oil tankers. It is a misconception, as some Western military leaders believe, that technology makes war cheaper and levels the playing field. Even if the unit cost of weapons decreases, the requirement for ever-growing quantities drives overall expenditure higher. Moreover, drones alone are insufficient: without reliable digital communications comparable to those provided by satellite networks such as Starlink, it is impossible to coordinate operations, gather intelligence, and maintain communication between units and command. This is why powers such as China are investing billions in this sector.

Technological transformation is accelerating the character of warfare, particularly through the integration of artificial intelligence, autonomous systems, and advanced digital capabilities. At the same time, the fundamental principles of war identified by classical theorists such as Clausewitz, Jomini, and Sun Tzu remain highly relevant. While technology can enhance military effectiveness, it cannot replace the human dimension of warfare, including leadership, morale, cohesion, determination, and the will to fight. The growing dependence on digital networks also increases vulnerability to cyber warfare, as network sabotage, power outages, and communication disruptions can significantly degrade operational effectiveness and create opportunities for enemy action. A compromised information system may neutralise critical military capabilities or severely limit their recoverability. Consequently, military innovation—from artificial intelligence to unmanned systems—must become a national priority. However, technological superiority alone is insufficient. The ability to mobilise and prepare forces, sustain combat power, and preserve morale will remain indispensable determinants of success.

Traditional doctrines must therefore be reassessed, and armed forces continuously adapted to the demands of an evolving operational environment. Yet adaptation should not be understood solely in technological terms. The most profound transformation must occur in military thinking, combining innovation with the enduring principles of military art. The experience of the Russia–Ukraine War demonstrates that success in modern warfare requires not only advanced technologies and flexible adaptation, but also effective leadership, resilient personnel, and strong societal and military morale. In an era of accelerated military change, victory will belong not simply to those who innovate fastest, but to those who successfully combine technological advantage with the timeless human factors that have shaped warfare throughout history.

METHODOLOGY

This analytical study is conducted within the framework of the Centre for Security and Military-Strategic Studies and supported by the Ministry of Defence of the Czech Republic under the Long-Term Development of Organisation – Armed Conflict (DZRO OZKON) programme. It builds upon a preceding analytical output published in 2024, which assessed the operating environment of the Russia–Ukraine war from February 2022 to autumn 2023 (Petráš 2024).

The present study extends this analysis to capture subsequent developments in the conflict's evolution, with particular emphasis on the increasing complexity of multi-domain operations (MDO) and the integration of kinetic and non-kinetic effects across the battlespace.

The methodological approach of this study is explicitly anchored in key NATO conceptual and doctrinal documents, in particular the Strategic Foresight Analysis 2023 (ACT 2023) and the NATO Warfighting Capstone Concept (ACT 2021). These documents identify critical drivers of future warfare development, including Cognitive Superiority, Power Projection, Cross-Domain Command, and Integrated Multi-Domain Defence, which collectively represent essential imperatives for maintaining operational advantage in a future operating environment within which Allied forces could be engaged.

In this context, the study aligns with NATO doctrinal terminology, notably the concepts of Multi-Domain Operations, hybrid warfare, and operations in contested and transparently observable environments. It adopts a system-of-systems analytical perspective, treating the operational environment as an interconnected and dynamic structure in which military and non-military effects emerge through interactions across multiple domains. Rather than viewing domains in isolation, the analysis emphasises their functional interdependence and the cumulative generation of operational effects across the entire battlespace.

Main Objective of the Study and Formulation of the Research Question

The main objective of this analytical study is to evaluate the evolution of the multi-domain operating environment in the Russia–Ukraine War between autumn 2023 and the turn of 2025–2026, identifying the principal changes in its operational characteristics, cross-domain interactions, and adaptation dynamics.

On the basis of this assessment, the study aims to formulate an analytically substantiated answer to the central research question: What implications do these changes have for the future of Euro-Atlantic security, particularly with regard to NATO's deterrence and defence posture, military capability development, defence planning, and strategic adaptation to contemporary large-scale warfare in a multi-domain operating environment?

Timeframe of the Study

The primary analytical timeframe covers the period from autumn 2023 to the end of 2025. This period was selected because it represents a distinct phase in the evolution of the Russia–Ukraine War, characterised by the transition from large-scale manoeuvre warfare to predominantly attritional operations, the aftermath of the Ukrainian counteroffensive, the intensification of long-range precision strike campaigns, the widespread employment of unmanned systems, and the consolidation of a mature multi-domain operating environment. During this period, the conflict demonstrated significant adaptation across the land, air, maritime, cyberspace, and space domains, providing a suitable basis for assessing changes in the operating environment and their implications for future warfare. However, recognising that several important operational and strategic developments occurred immediately after the end of 2025, the analysis is supplemented, where appropriate, by selected developments extending into the beginning of 2026. These references are included only where they contribute to a more comprehensive understanding of the evolution of the operating environment or substantiate analytical conclusions concerning the future of Euro-Atlantic security.

Analytical Framework and Research Design

The analytical framework is based on a systematic search and critical review of open-source materials. Sources were identified through targeted searches of main databases (see Table 1), official NATO and governmental publications, defence think tank reports, and peer-reviewed literature. Selection was guided by their relevance to the study's objectives, analytical credibility, methodological transparency, and their contribution to understanding the evolution of the Russia–Ukraine War and its implications for Euro-Atlantic security.[1]

Table 1: List of Main Databases Used for Literature Research

Common Security and Defence Policy (CSDP) EU Statistics and Data	https://ec-europa-eu.libguides.com/security-and-defence/statistics/eu
US Defense Technical Information Center	https://discover.dtic.mil/
UK Defence and Armed Forces	https://www.gov.uk/defence-and-armed-forces
Institut de Recherche Stratégique de l'Ecole Militaire (IRSEM)	https://www.irsem.fr/
Fondation pour la recherche stratégique (FRS)	https://www.frstrategie.org/
NATO Library	https://natolibguides.info/natolibrary
Center for Strategic and International Studies (CSIS)	https://www.csis.org/topics/defense-and-security
NATO Science and Technology Organization (NATO STO)	https://www.sto.nato.int/Pages/default.aspx

[1] The detailed methodological documentation, including source-selection criteria, analysed content, coding scheme, and reliability scale applied for assessing the findings, could not be included in this publication due to its scope limitations. These materials are available from the author upon request.

These sources provide both theoretical and empirical perspectives on the evolving character of warfare, including attritional conflict dynamics, technological adaptation, and the growing role of space-enabled and cyber-enabled capabilities. The analytical process integrates:

- structured literature review,
- directed qualitative content analysis,
- phase-based operational assessment, and
- cross-domain systems analysis.

A central pillar of the methodology is comparative analysis, which examines interactions between operational domains within the Ukrainian theatre of operations. This approach reflects NATO's doctrinal shift towards converged, cross-domain effects generation, in which operational advantage is achieved by integrating capabilities across domains rather than by isolated domain superiority.

The study distinguishes five primary domains:

- Land domain, assessed through attritional dynamics, force engagement patterns, and defensive systems development;
- Air domain, focusing on air denial strategies, unmanned aerial system (UAS) employment, and precision strike operations;
- Maritime domain, examining control and denial dynamics in the Black Sea operational environment;
- Cyber domain, addressing network disruption operations, critical infrastructure targeting, and digital interference activities;
- Space domain, evaluating ISR support functions, satellite-enabled communications, and dependency on space-based systems.

Each domain is first analysed independently to identify its internal operational logic, capability-employment patterns, and adaptation mechanisms. Subsequently, the findings are integrated into a cross-domain interaction matrix, which serves as the study's principal analytical instrument. This matrix enables identification of:

- Synergistic effects, such as cyber operations contributing to kinetic targeting or ISR enhancement;
- Cross-domain dependencies, particularly reliance on space-based assets for targeting cycles and command-and-control continuity;
- Feedback loops, whereby battlefield adaptation influences doctrinal development in cyber, electronic warfare, and unmanned systems employment.

This structure reflects NATO's emphasis on convergent effects-based operations, in which operational outcomes emerge from synchronised activity across multiple domains rather than dominance within a single domain.

The analytical framework is further grounded in the MDO concept (Trusch 2025), which serves as the principal interpretive lens for assessing operational behaviour. The study does not focus on isolated platforms or tactical engagements; instead, it examines how capabilities are integrated to generate simultaneous systemic operational and strategic effects across domains. Attention is given to identifying:

- areas where observed battlefield dynamics validate existing NATO assumptions on MDO;
- areas where empirical evidence suggests the need for doctrinal adaptation;
- emerging dependencies between cyber, space, and kinetic systems in contested environments.

The integration of qualitative and structured analytical methods enables interpretation of the Russia–Ukraine conflict as a multi-domain adaptive system of warfare, in which operational effectiveness is determined by the interaction of kinetic and non-kinetic effects across domains. The framework facilitates the identification of key drivers shaping contemporary warfare while simultaneously generating insights relevant to NATO capability development and operational planning.

The analytical process culminates in a structured expert assessment of the conflict's evolution and operational characteristics, derived from the qualitative analysis of selected sources. This assessment synthesises the principal characteristics of the evolving operating environment and provides an evidence-based evaluation of their implications for Euro-Atlantic security, NATO capability development, defence planning, force generation, and operational preparedness. The findings are assessed against NATO doctrinal priorities. The study also addresses the implications of operating in a transparent and persistently contested battlespace, characterised by continuous surveillance, long-range precision strike capabilities, and cross-domain competition.

Limitations

The study acknowledges inherent limitations of Open-Source Intelligence (OSINT)-based analysis, including information asymmetry, selective reporting, and potential bias in wartime information environments. The absence of classified operational data constrains insight into command intent and decision-making processes. Furthermore, observable cyber- and space-related effects may be disproportionately represented compared with unobserved or covert activities. Attribution in cyber and information warfare remains inherently uncertain; therefore, all findings in these domains are assessed using calibrated confidence levels and cross-source validation.

1. DECISIVE PHASES AND OPERATIONAL DYNAMICS OF THE RUSSIA–UKRAINE WAR

This section provides a structured overview of the decisive moments and key operational phases of the Russia–Ukraine War during 2024–2025, which serves as the analytical foundation for the subsequent assessment of the operational environment. The analysis is organised chronologically and reflects the evolution of the conflict across multiple domains, with particular emphasis on shifts in operational initiative, force employment, and the interaction between kinetic and non-kinetic effects within the battlespace.

The identification of decisive moments and operational phases presented in this chapter is primarily based on analytical outputs developed by the Institute for the Study of War (ISW), whose assessments provide a consistent and methodologically robust framework for understanding the evolution of the conflict.

The selected phases capture critical developments that affect the battlespace framework, including changes across the physical, virtual, and cognitive dimensions of warfare. These developments are analysed through the lens of core doctrinal concepts such as operational reach, freedom of manoeuvre, sustainment, force generation, and the balance between offensive and defensive operations. The period under examination illustrates the transition from manoeuvre-oriented operations towards a predominantly attritional operational approach, in which firepower, endurance, and the ability to sustain combat operations over time became decisive factors.

The identified phases highlight the interplay between tactical actions and strategic effects. Key events—such as major offensive operations, cross-border manoeuvre activities, and the expansion of deep-strike campaigns—demonstrate how localised engagements can produce wider operational and strategic consequences. In particular, the increasing importance of long-range precision fires, Unmanned Aerial Systems (UAS), and strikes against critical infrastructure underscores the conflict's multi-domain character and the growing role of strategic interdiction in shaping operational outcomes.

Furthermore, this section reflects the centrality of force generation, sustainment capacity, and combat resilience in a high-intensity conflict. The ability of both belligerents to generate, regenerate, and effectively employ combat power—while simultaneously contesting the adversary’s war-sustaining systems—emerges as a critical determinant of operational success.

Overall, the overview presented in Table 2 is both descriptive and analytical. By identifying decisive phases and key inflexion points, it establishes a coherent framework for evaluating the operational environment, including threat capabilities, vulnerabilities, and the evolving balance of power within the theatre of operations.

Table 2: Decisive Phases of the Russia–Ukraine War (2024–2025) (Author)

Phase	Key Events	Operational Characteristics	Strategic / Operational Outcome
Russian Offensive in Donbas (Jan–Mar 2024)	Intensified Russian attacks; capture of Avdiivka (17 Feb 2024)	Massed fires, glide bombs, UAS; Ukrainian shortages (ammo, AD); defence-in-depth	Russia gains the initiative; attritional pressure dominates; a key Ukrainian defensive node is lost
Ukrainian Cross-Border Operation (Kursk) (Aug–Sep 2024)	Ukrainian incursion into the Kursk region (~10,000 troops)	Mobile manoeuvre + long-range strikes; targeting logistics/C2 nodes; Russian counterattacks	Limited territorial success but strategic signalling effect; forces Russia to divert resources
Deep-Strike Escalation (Sep–Nov 2024)	Use of ATACMS / Storm Shadow into Russia; escalation of infrastructure strikes	Expansion of long-range precision strikes; both sides target logistics, energy, and C2	Conflict becomes multi-domain & depth-focused; strategic interdiction rises in importance
Russian Offensive & Territorial Gains (Nov–Dec 2024)	Russian pressure on Pokrovsk, Chasiv Yar; continued gains (~4,168 km² in 2024)	Sustained mobilisation, numerical advantage, attritional assaults	Russia retains initiative; Ukraine under manpower/logistics strain; attrition intensifies
Pivotal Event – Loss of Avdiivka (Feb 2024, cross-phase)	Ukrainian withdrawal from key stronghold	Russian 3:1 local superiority; systematic firepower + UAS	Major operational & psychological turning point; enables further Russian advances
Kursk Salient & Russian Counteroffensive (Jan–Mar 2025)	Russian recapture of ~86% of Ukrainian-held Kursk territory	Coordinated counteroffensive, high tempo, multi-axis manoeuvre	Russia restores initiative; demonstrates limits of Ukrainian cross-border operations
Russian Air & Missile Campaign (Summer 2025)	Large-scale strikes on AD systems, energy, and industry	Mixed use of drones + missiles to exhaust air defence; cost-exchange strategy	Partial success; Ukraine adapts via dispersion & resilience; attrition deepens
Consolidation of Russian Initiative (Autumn 2025)	Multi-axis offensives; ~19% of Ukraine controlled	Persistent offensive pressure; Ukrainian defensive posture dominates	Strategic balance shifts toward Russia; Ukraine focuses on defence and force preservation
Consolidation of Attritional Environment (Autumn 2025–Winter 2026)	Stabilisation with continued deep strikes	Weather limits manoeuvre; sustained fires and infrastructure attacks	War fully transitions to protracted attritional conflict; Russia dictates tempo

1.1 Russian Offensive Operations in the Donbas (January–March 2024)

The beginning of 2024 was marked by the resumption of Russian offensive operations following the limited outcomes of the Ukrainian counter-offensive conducted during the summer and autumn of 2023. The Russian Federation sought to exploit the cumulative effects of Ukrainian force exhaustion, ammunition shortages, and delays in the delivery of international military assistance. The Donbas remained the principal operational focus, where Russian forces pursued a strategy of progressive attrition to degrade Ukrainian defensive capabilities and secure key terrain.

The most intense combat activity occurred in the Avdiivka sector, which had become a major defensive stronghold within Ukraine's defensive architecture. Russian forces conducted a deliberate offensive operation based on the integrated employment of massed indirect fires, including artillery and multiple-launch rocket systems, precision-guided aerial munitions such as FAB-1500 glide bombs, and extensive use of Unmanned Aerial Systems (UAS), including Lancet loitering munitions. This approach enabled the systematic degradation of Ukrainian defensive positions, command-and-control arrangements, logistics nodes, and sustainment infrastructure.

During this period, Ukrainian forces faced significant operational constraints. Limited stocks of artillery ammunition and precision-guided munitions, including those employed by HIMARS (High Mobility Artillery Rocket Systems), combined with shortages of air-defence interceptors for systems such as Patriot, reduced Ukraine's capacity to conduct long-range precision engagements and counter Russian air-delivered strike operations. Consequently, Ukrainian forces increasingly relied on asymmetric capabilities, particularly First-Person View (FPV) strike drones, while emphasising a defence-in-depth approach based on fortified positions, trench networks, and prepared defensive belts. The culmination of this phase was the Russian capture of Avdiivka on 17 February 2024. Following months of sustained combat and progressive envelopment of the urban area, Ukrainian forces conducted a withdrawal to avoid encirclement and preserve combat power. The capture of Avdiivka represented a significant tactical success for Russian forces, strengthening their position in eastern Donbas and creating favourable conditions for subsequent offensive operations.

Overall, the first phase of 2024 was characterised by Russian operational initiative and the systematic application of attritional pressure. Russian advances were enabled by superiority in massed fires, the effective integration of emerging technologies, and sustained force generation capacity. In contrast, Ukraine focused on stabilising the frontline, preserving combat effectiveness, and mitigating losses while awaiting additional international military assistance and the replenishment of critical capabilities.

1.2 Cross-Border Operations in the Kursk Region (August–September 2024)

During the summer of 2024, Ukraine shifted toward more offensive and operationally innovative activities aimed at altering the conflict's dynamics and imposing new dilemmas on the Russian command. On 6 August 2024, Ukrainian forces launched a limited cross-border offensive operation into Russia's Kursk region. The operation involved approximately 10,000 personnel and was designed to disrupt Russian rear-area activities, degrade critical logistics infrastructure, and compel the Russian Federation to reallocate forces from priority operational sectors within Ukraine.

The operation combined highly mobile manoeuvre elements with long-range precision-strike capabilities. Ukrainian forces employed mechanised formations equipped with T-80 main battle tanks, mobile assault elements, and HIMARS to engage high-value targets within the Russian operational rear. Priority targets included ammunition storage sites, command-and-control nodes, logistics facilities, and transportation infrastructure supporting Russian operations in Ukraine. By targeting these critical enablers, Ukraine sought to disrupt Russian sustainment networks, complicate force movement, and impose additional operational burdens on Russian military planners.

The Russian response was rapid and robust. Russian forces reinforced the Kursk region by redeploying additional combat formations and initiated counteroffensive operations supported by airpower and long-range strike assets. A significant role was played by Su-34 fighter-bombers conducting air-to-surface strike missions against advancing Ukrainian formations, while Kalibr land-attack cruise missiles were employed against Ukrainian logistics hubs, staging areas, and force concentration points. Through a combination of reinforcement, counterattacks, and sustained fire support, Russian forces gradually regained control of much of the territory that Ukrainian forces had temporarily seized.

Although the operation achieved only limited and temporary territorial gains, its strategic significance exceeded its geographic scope. The incursion demonstrated Ukraine's ability to project combat power onto Russian territory, thereby challenging assumptions regarding the security of Russia's operational rear areas. The operation also compelled Russian military authorities to devote additional resources to homeland defence and border security, creating competing demands for forces already committed to ongoing offensive operations in Ukraine.

Consequently, the second phase of 2024 marked a notable shift in the operational balance of the conflict. Ukraine regained a degree of initiative not through a large-scale breakthrough operation, but through a limited-objective manoeuvre operation designed to generate disproportionate strategic, operational, and psychological effects relative to the forces committed.

1.3 Deep-Strike Operations and Strategic Escalation (September–November 2024)

The third phase of 2024 was characterised by a significant escalation of the conflict and a further expansion of deep-strike operations within the broader strategic battlespace. A key development occurred on 17 September 2024, when the U.S. Administration authorised Ukraine to employ the Army Tactical Missile System (ATACMS) against selected military objectives within the internationally recognised territory of the Russian Federation. Subsequently, Western political support increasingly enabled Ukraine to employ certain Western-supplied long-range strike capabilities, including Storm Shadow cruise missiles, against military targets within Russian territory. This development represented a significant shift in previous restrictions governing the employment of Western-provided capabilities, which had largely limited their use to operations within Ukrainian territory and occupied areas.

Ukraine rapidly integrated these capabilities into its deep-strike campaign. Using long-range precision-guided weapons, Ukrainian forces conducted attacks against high-value military targets located in the operational and strategic depth of the Russian Federation. Priority targets included air bases, ammunition storage facilities, logistics hubs, command-and-control (C2) nodes, and critical transportation infrastructure, particularly railway junctions that support force movement and sustainment operations. These strikes sought to disrupt Russian operational logistics, degrade force generation and reinforcement processes, and impose additional constraints on Russian operational planning and execution.

The Russian Federation responded through a further intensification of its strategic strike campaign against Ukrainian critical infrastructure. Emphasis was placed on targeting the national energy sector, including power-generation facilities, electrical substations, and transmission networks, with the objective of degrading Ukraine’s war-sustaining capacity, reducing societal resilience, and generating broader economic effects. These attacks combined the mass employment of one-way attack UAS, notably Shahed systems, with advanced long-range precision-strike capabilities, including the Kh-47M2 Kinzhal air-launched ballistic missiles, which were employed against heavily defended and high-priority targets.

As a result, the conflict increasingly became a contest of reciprocal deep-strike operations that extended beyond the immediate frontline. While ground combat operations remained decisive in determining territorial control, the growing importance of long-range precision fires, one-way attack UAS, and attacks against critical military and civilian infrastructure highlighted the expanding role of strategic interdiction and infrastructure warfare in shaping operational outcomes.

Consequently, the third phase of 2024 represented a period of both geographic and strategic expansion of the conflict. Both belligerents increasingly sought to achieve military advantage by degrading the adversary's logistics networks, defence-industrial capacity, energy infrastructure, and broader war-sustaining systems. This development further reinforced the conflict's multi-domain character and underscored the growing importance of deep-strike capabilities in contemporary high-intensity warfare.

As illustrated in Figure 1, in August 2024, Ukraine launched over 1,000 drones against Russia's military targets; in July 2025, 3,000; and in March 2026, 7,000, according to data from both Ukraine's Air Force and the Russian Ministry of Defence. Ukraine managed to overtake Russia in 2026 in terms of long-range drone strikes.

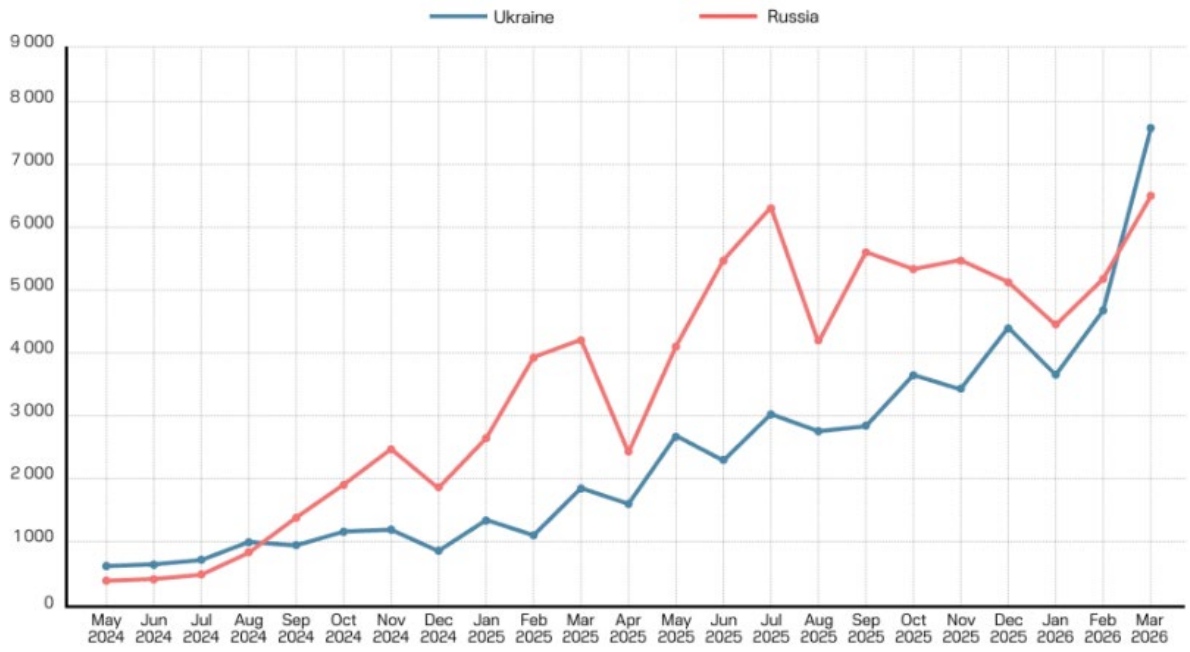

Figure 1: Long-Range Drone Strikes Russia vs Ukraine (Place 2026)

1.4 Russian Offensive and Territorial Gains (November–December 2024)

The final phase of 2024 was characterised by renewed Russian operational pressure along key sectors of the Donbas frontline. Russian forces concentrated their main effort on the Pokrovsk axis and the Chasiv Yar area, which is assessed as operationally significant terrain due to its industrial capacity, transportation nodes, and role in the Ukrainian defensive depth. The objective of these operations was to penetrate Ukrainian defensive belts, disrupt their continuity, and expand Russian control over critical terrain within the Donetsk operational area. Russian operational momentum during this period was primarily enabled by sustained force generation and numerical superiority, reinforced by continued mobilisation and the integration of newly formed units. Although the combat effectiveness of these formations varied, their employment alongside established units enabled Russia to maintain persistent offensive pressure.

This was further supported by continued dominance in indirect fire and the integrated use of air support, enabling Russian forces to conduct systematic fire preparation followed by incremental infantry-based assaults in accordance with an attritional force-employment model. Ukraine entered this phase with partially enhanced long-range strike capabilities, particularly through the introduction and increased availability of extended-range systems enabling strikes against Russian operational depth. While these capabilities imposed additional friction on Russian command-and-control, logistics, and sustainment systems, they did not fully offset the sustained pressure exerted along the frontline. Ukrainian defensive operations were further constrained by personnel fatigue, limited force regeneration cycles, extended rotational timelines, and persistent shortfalls in manpower and materiel reserves.

According to estimates (ISW 2026a), Ukraine experienced territorial losses of approximately 4,168 km² in 2024, with a significant proportion occurring in the second half of the year (see Figure 2). These developments reflected both sustained Russian offensive pressure and enduring structural challenges within Ukrainian force generation, sustainment capacity, and the maintenance of combat effectiveness under conditions of prolonged high-intensity attrition.

A further critical factor was the onset of winter conditions combined with continued Russian long-range strikes against Ukraine’s energy infrastructure. Sustained attacks on power-generation facilities, transmission networks, and associated critical infrastructure caused widespread disruptions to the electrical supply. These effects negatively impacted not only civilian resilience but also defence-industrial output, logistics throughput, and the sustainment of military operations. Adverse environmental conditions further compounded operational stress across Ukrainian formations.

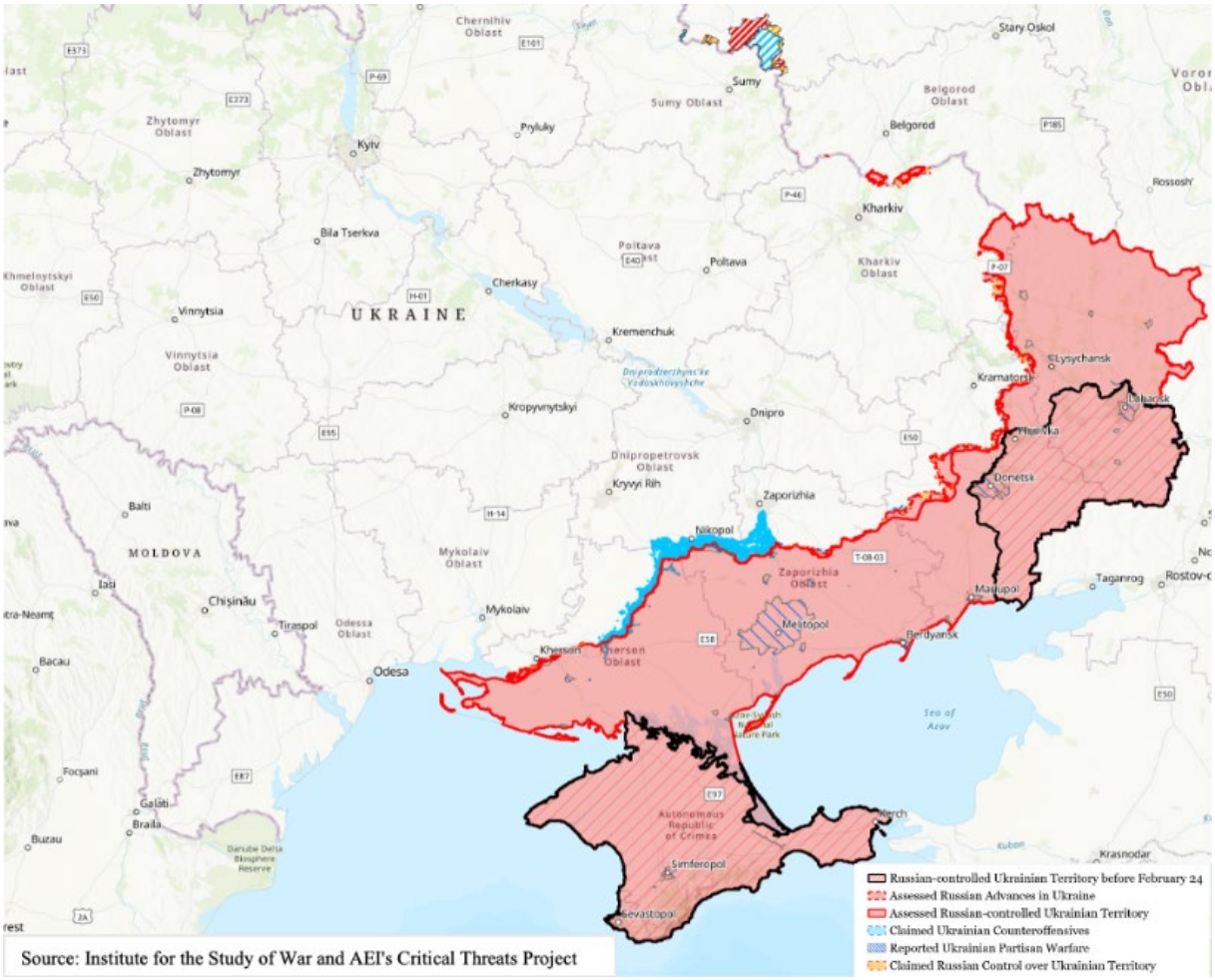

Figure 2: Russian Territorial Gains in November–December 2024 (ISW 2026a)

In sum, the fourth phase of 2024 was characterised by Russia's retention of the operational initiative and incremental territorial gains at high cost. Ukraine, in turn, faced an accumulation of operational, logistical, and strategic pressures that underscored the conflict's protracted nature and reinforced the centrality of attrition as the dominant framework for conducting contemporary high-intensity warfare.

1.5 Ukrainian Defence Pivotal Moment - The Loss of Avdiivka (17 February 2024)

The most significant turning point for Ukraine in 2024 was the withdrawal from Avdiivka on 17 February 2024. This event constituted not only a major tactical setback but also an important operational and strategic inflexion point, with notable psychological effects on the broader conduct of the campaign.

Avdiivka had long functioned as a key Ukrainian defensive strongpoint within the Donetsk operational area, as shown in Figure 3. Its location in close proximity to Donetsk city provided a forward defensive position that constrained Russian freedom of manoeuvre and enabled Ukrainian forces to interdict key ground lines of communication and logistical routes supporting Russian operations. The loss of this position consequently created favourable conditions for further Russian offensive action directed westwards along the Donbas axis.

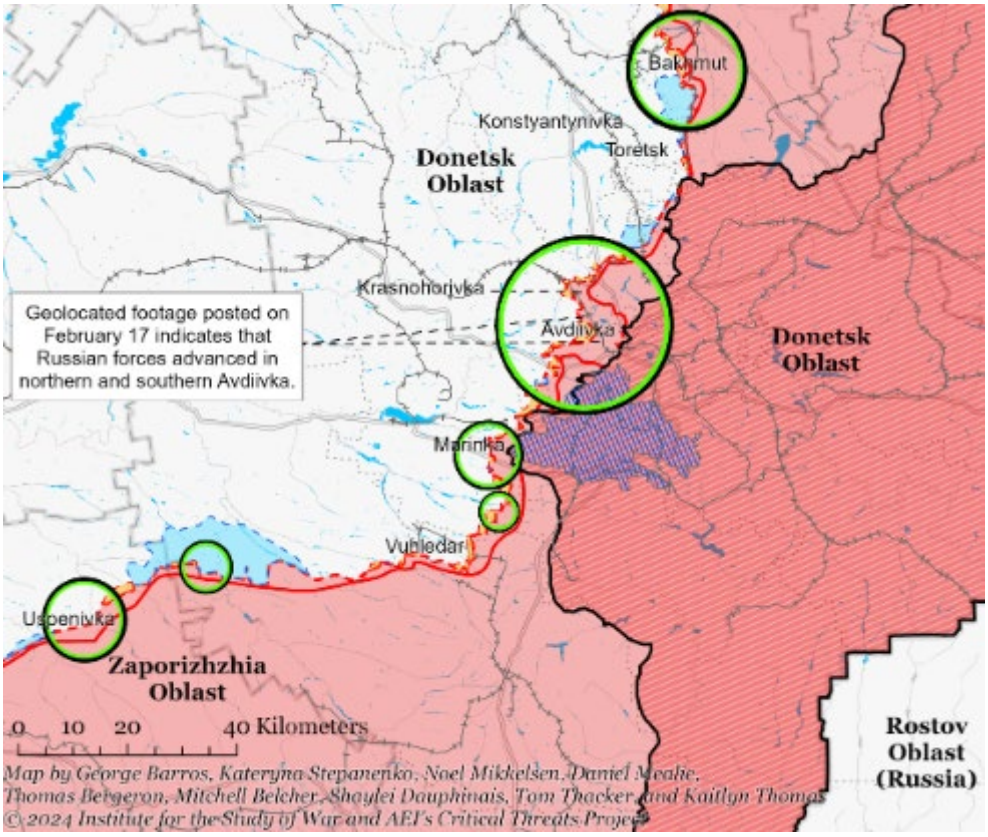

Figure 3: Avdiivka – operational situation as in February 2024 (ISW 2024)

A decisive factor in the loss of Avdiivka was the pronounced imbalance in the force ratio at the tactical and operational levels. Ukrainian forces were confronted by numerically superior Russian formations, assessed at approximately a three-to-one advantage in localised combat power, while simultaneously experiencing critical shortages of artillery ammunition, including munitions for HIMARS and NATO-standard artillery systems.

These shortfalls were exacerbated by delays in the provision of Western military assistance, which constrained Ukraine's ability to sustain adequate rates of fire and maintain defensive endurance under continuous pressure. Russian forces concentrated significant combat power in the sector, including an estimated force grouping of approximately 40,000 personnel. The operation was characterised by sustained attritional warfare, with extensive use of massed indirect fires and integrated air-delivered effects. A key component of the Russian fire plan involved the employment of FAB-1500 glide bombs[2], enabling precision strikes against fortified Ukrainian defensive positions and contributing to the systematic degradation of layered defensive belts. Concurrently, Lancet loitering munitions were employed in a persistent interdiction role against Ukrainian armoured vehicles, artillery systems, and other high-value assets, further reducing Ukrainian combat effectiveness.

The operational consequences of the withdrawal from Avdiivka were multi-layered. At the tactical level, Ukrainian forces were compelled to abandon prepared defensive positions and transition to secondary defensive lines with reduced fortification density. At the operational level, Russian forces gained improved positioning for subsequent offensive actions within the Donetsk axis, enhancing their ability to sustain pressure against Ukrainian defensive formations. Strategically, the loss reinforced the effectiveness of Russia's attrition-based operational approach and highlighted the cumulative effects of sustained battlefield pressure, while also adversely affecting Ukrainian morale at both the military and societal levels.

The loss of Avdiivka represents a critical milestone in the 2024 campaign. It exposed the limits of Ukrainian force sustainability under conditions of prolonged attritional warfare and underscored the effectiveness of Russian force concentration and systematic application of firepower in degrading prepared defensive systems. This event significantly influenced the subsequent operational trajectory of the conflict.

[2] The FAB-1500-2600TS is 1,500-kilogram aerial bomb modified to carry out precision strike attack at long ranges using glide modification kit. The new long-range, glide bomb is intended to be used during the Special Military Operation in Ukraine beginning in April or May 2023. Besides, some wing kits the bomb may feature GLONASS satellite navigation to achieve enhanced accuracy. The ODAB-1500 is a fuel-air-explosive (FAE) bomb variant.

1.6 Mobilisation, Force Generation, and Desertion Dynamics in 2024

In 2024, force-generation capacity, mobilisation systems, and personnel sustainability emerged as decisive factors, alongside kinetic combat operations, in shaping the conflict's overall trajectory. The ability of both belligerents to generate, regenerate, and sustain combat forces directly influenced operational endurance in a protracted attritional environment. In parallel, increasing strain on human resources, coupled with growing indicators of morale degradation and disciplinary breakdowns, affected force effectiveness at both tactical and operational levels.

On the Russian side, force generation was built upon the partial mobilisation conducted in 2022, during which approximately 300,000 personnel were called up. Throughout 2024, the Russian Federation expanded its force pool through sustained recruitment campaigns, financial incentives, contract-based enlistment, and regional mobilisation measures. According to New Eurasian Strategies Centre estimates (Lough 2024), these efforts generated an additional 200,000 to 250,000 personnel. As a result, the total Russian force group associated with operations against Ukraine is assessed at approximately 600,000 to 700,000 personnel, of which an estimated 300,000 to 450,000 were committed to frontline combat formations.

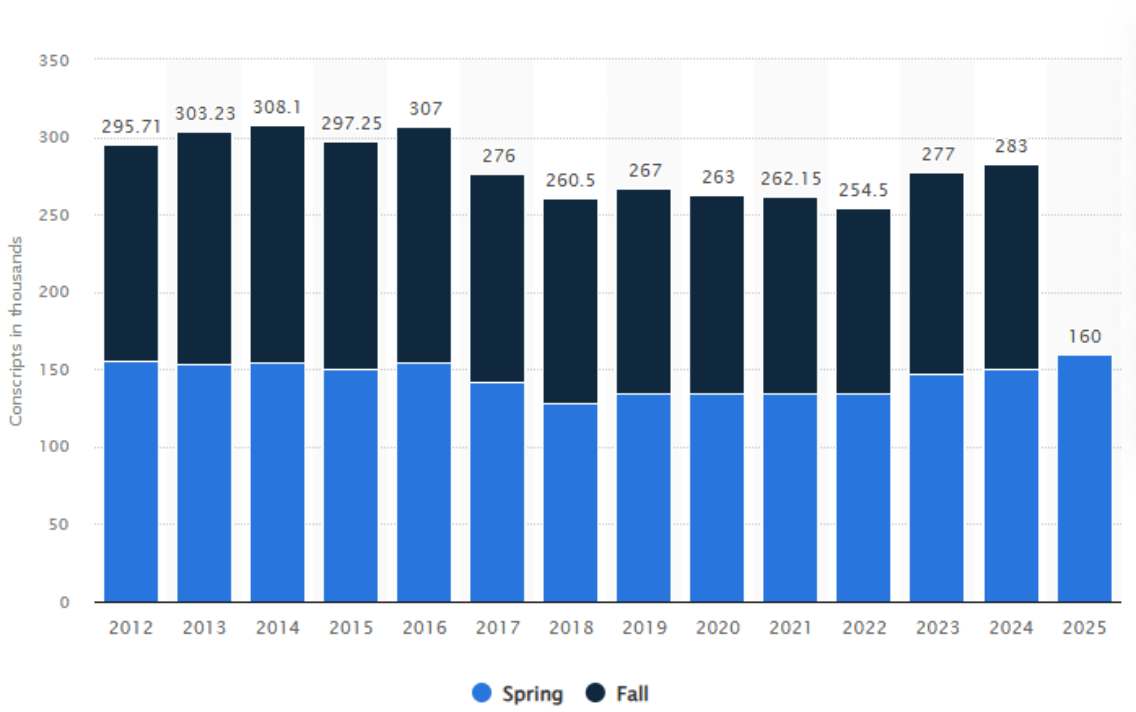

Figure 4: Number of military conscripts in Russia from 2012 to 2025 (Statista 2026)

A total of 160,000 conscripts were called up during Russia's spring 2025 draft, followed by a further 135,000 during the autumn 2025 draft. Over the past decade, the highest annual conscription was recorded in 2014, at 308,100 (Statista 2026). This force density provided Russia with a significant quantitative advantage, particularly in attrition warfare, where operational success depends on the ability to absorb losses, rotate units, and sustain continuous pressure along extended frontlines. Although the combat effectiveness of newly generated formations was uneven, their numerical mass enabled a sustained offensive tempo and facilitated the systematic application of attritional pressure against Ukrainian defensive positions.

Ukraine, by contrast, faced more constrained conditions for force generation. In 2024, Ukrainian combat strength on the front lines is estimated at 200,000 to 300,000 personnel, significantly lower than Russian forces. In response to sustained personnel losses and the need to regenerate combat-effective units, the Ukrainian government implemented martial law provisions and adjusted mobilisation parameters, including reducing the conscription age threshold to 25 years. These measures were intended to expand the available mobilisation base and stabilise force-generation pipelines but also reflected the increasing strain on national human resources.

As the conflict persisted, indicators of force exhaustion became more pronounced. Reports of draft evasion increased alongside documented cases of desertion from operational units. These phenomena were associated with extended deployment cycles, limited opportunities for rotation and recuperation, psychological fatigue, and uneven levels of equipment availability across units. Together, these factors contributed to challenges in maintaining unit cohesion and sustained combat effectiveness.

Overall, developments in 2024 demonstrated that, alongside technological adaptation and tactical evolution, force generation and personnel sustainability remain decisive determinants of operational effectiveness. While the Russian Federation was able to leverage its demographic depth and mobilisation mechanisms to maintain numerical superiority, Ukraine faced progressively increasing constraints in force replenishment, personnel retention, and the maintenance of combat morale under conditions of sustained high-intensity attritional warfare.

1.7 The Kursk Salient and Russian Operational Initiative (January–March 2025)

During the opening months of 2025, most frontline sectors remained relatively static, although indicators of progressive degradation in Ukrainian defensive resilience became increasingly apparent. This trend was shaped significantly by the outcomes of the preceding year, particularly the Ukrainian cross-border operation into the Kursk region, which temporarily altered the local operational balance and compelled Russian forces to adjust force posture and prioritisation of operational reserves. Following the Ukrainian incursion initiated in August 2024, Ukrainian forces established a forward salient on Russian territory, including the seizure of Sudzha, thereby creating a limited but operationally and politically significant bridgehead. This Kursk Salient constituted both a tactical success and a strategic signalling effect, demonstrating Ukraine's capacity for limited cross-border manoeuvre operations and imposing a requirement on the Russian Armed Forces to retain and allocate combat forces for homeland defence tasks.

The Ukrainian presence in the area persisted for approximately seven months, during which Russia conducted systematic shaping operations and a buildup of forces in preparation for a counteroffensive. The decisive shift occurred in March 2025, when Russian forces launched a rapid, coordinated counteroffensive to eliminate the salient and restore the integrity of the state border. Russian units achieved accelerated territorial recovery, regaining more than 86% of the area previously under Ukrainian control (approximately 1,100 km²) by 13 March 2025. The operation was characterised by a high operational tempo, coordinated multi-axis manoeuvre, and the sequential recapture of multiple settlements, including Sudzha, the principal node of the Ukrainian forward position.

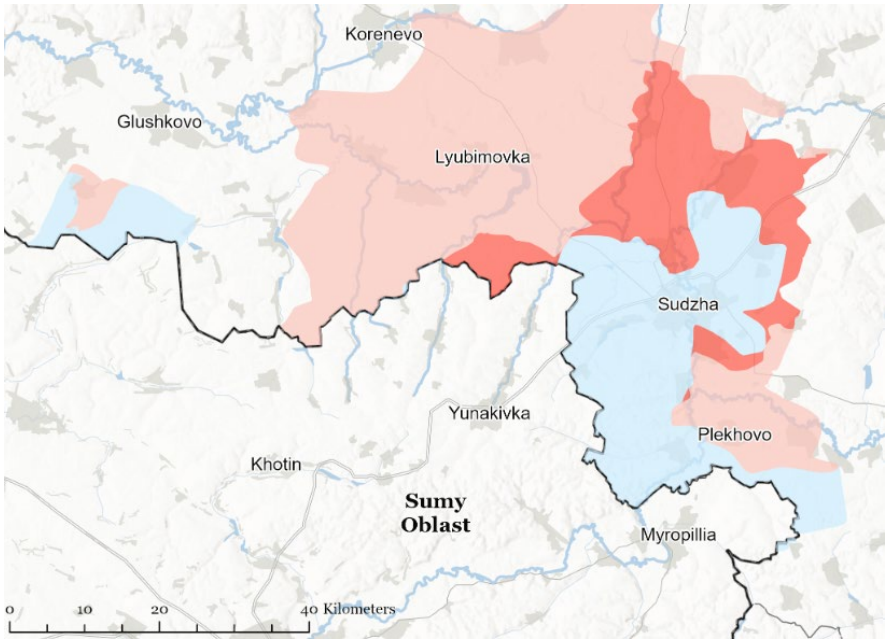

Figure 5: Assessed Russian Advances in Kursk Salient in March 2025 (ISW 2025b)

Ukrainian forces withdrew under pressure to avoid operational encirclement and further degradation of combat power. The withdrawal was accompanied by significant personnel losses, including the capture of several hundred Ukrainian service members, reflecting the intensity and compressed nature of the retrograde operation. Russian forces subsequently exploited the information environment, with senior political leadership publicly highlighting the outcome and framing the operation as the restoration of territorial integrity and the elimination of the Ukrainian forward presence on Russian territory.

In parallel, Russian forces initiated limited forward security operations beyond the international border into Ukraine's Sumy region, where forward elements began establishing temporary defensive positions. These actions were presented by the Russian side as part of a broader effort to establish a forward security zone to mitigate the risk of future cross-border incursions and enhance the depth of defence along the border. Overall, the Kursk Salient episode demonstrated both the operational utility and inherent limitations of limited-objective cross-border operations conducted without sustained force generation, logistical depth, and long-term reserve capacity. The subsequent Russian counteroffensive restored local operational control, re-established the Russian initiative at the tactical and operational levels, and generated a favourable informational and strategic effect. This phase, therefore, marked a transition from relative operational stagnation to a renewed Russian initiative in both the local battlespace and the wider strategic context of the conflict.

1.8 Russian Air and Missile Offensive Campaign (Summer 2025)

The Russian air and missile campaign conducted during the summer of 2025 constituted a central component of a broader operational approach aimed at degrading Ukraine’s defensive capacity and reducing the effectiveness of its defence-industrial base. The campaign pursued two principal operational objectives: first, the systematic depletion and saturation of Ukrainian air defence systems; and second, the progressive degradation of critical nodes within Ukraine’s defence-industrial and sustainment infrastructure.

The first objective was pursued through sustained, high-tempo air and missile strikes designed to impose continuous pressure on Ukrainian Integrated Air Defence System (IADS) elements and compel the expenditure of limited stocks of advanced surface-to-air missile interceptors, largely supplied by Western partners. Russian forces employed a mixed-strike-package approach, combining large numbers of one-way attack UAS, particularly Shahed-type systems, with higher-cost precision-guided munitions.

This force mix was intended to create a cost-exchange imbalance, forcing Ukrainian air defence systems to engage lower-cost aerial threats with disproportionately expensive interceptors, thereby accelerating the depletion of available stocks and straining air defence readiness.

The second operational objective focused on the deliberate targeting of Ukraine's war-sustaining capacity. Russian long-range strike assets were employed against energy-generation and transmission infrastructure, ammunition storage sites, repair and maintenance facilities, and defence-industrial production nodes. These strikes caused measurable degradation of national energy capacity, with cascading effects on civilian infrastructure, military logistics, and defence production. In parallel, disruption of selected industrial programmes, including elements of domestic missile development, reflected the broader intent to constrain Ukraine's long-term force generation and capability development.

Despite the intensity of this campaign, its overall operational effectiveness remained partial rather than decisive. Ukrainian forces demonstrated a high degree of adaptive resilience, particularly through the dispersal and segmentation of defence-industrial production. The emergence of decentralised production networks, including a proliferation of small and medium-sized enterprises focused on UAS and related technologies, reduced vulnerability to area-based strikes and mitigated the effects of the loss of individual facilities within a distributed production architecture.

In addition, the partial relocation of selected production capacity outside Ukrainian territory helped maintain output amid persistent strikes. Western military assistance remained a critical enabling factor, particularly in offsetting losses of ammunition stocks and air defence interceptors. Concurrently, broader allied initiatives aimed at scaling up ammunition production, including within the European defence industrial base, sought to mitigate long-term disparities in materiel consumption rates and sustain Ukraine's operational endurance.

Overall, the Russian air and missile offensive in the summer of 2025 functioned as a sustained coercive pressure mechanism within a broader attritional framework. While it inflicted significant damage on infrastructure and imposed persistent operational strain, it did not achieve a decisive reduction in Ukrainian combat capability. Instead, the campaign further reinforced the conflict's adaptive character, in which Russian efforts to generate cumulative destructive effects were met with Ukrainian dispersion, redundancy, and external support mechanisms, thereby deepening the war's fundamentally attritional nature.

1.9 Consolidation of Russian Operational Initiative in Autumn 2025

With the onset of autumn 2025, a discernible shift occurred in the overall operational balance in favour of the Russian Federation. Following the period of Ukrainian offensive initiatives in 2023 and early 2024, Russian forces progressively restored operational stability, reconstituted combat effectiveness, and regained the strategic initiative. Throughout 2025, this trend evolved into a series of coordinated, multi-axis offensive operations characterised by incremental advances and sustained attritional pressure against Ukrainian defensive formations.

Russian forces conducted simultaneous offensive operations along multiple axes of advance, thereby compelling Ukrainian forces to disperse combat power and adopt a predominantly defensive posture. Ukrainian command structures increasingly prioritised defensive consolidation, delay operations, and the reinforcement of threatened sectors, rather than the planning and execution of large-scale manoeuvre offensives. This posture reflected constraints in force generation, limited operational reserves, and cumulative combat losses, which necessitated the employment of remaining high-readiness formations in sectors assessed as most critical.

From a territorial perspective, Russian forces consolidated control over approximately 19% of Ukrainian territory, including Crimea, and established control over more than two-thirds of the Donetsk oblast. While key urban centres such as Kramatorsk, Sloviansk, Zaporizhzhia, and Dnipro remained under Ukrainian control, Russian operational activity indicated a deliberate effort to progressively isolate them by interdicting lines of communication and eroding adjacent defensive nodes. Intensified combat in the Kostyantynivka area, a key operational node on the approaches to Kramatorsk, together with the capture of subsidiary settlements, reflects a broader Russian intent to disrupt Ukrainian operational depth and set conditions for potential encirclement of major defensive hubs in the Donbas.

On the northeastern axis, potential Russian advances towards Kupiansk, coupled with expansion of the security buffer zone in the Sumy direction, would further constrain Ukrainian cross-border manoeuvre options while enhancing the depth of defence for the Belgorod and Kursk operational sectors. These areas simultaneously provide favourable staging conditions for continued Russian offensive activity.

In the southern operational direction, Russian forces focused on consolidating the land corridor between Donbas and Crimea. Following unsuccessful Ukrainian attempts to conduct offensive operations towards Melitopol, Russian forces continued offensive pressure towards Zaporizhzhia, with the objective of securing operational continuity, strengthening logistics sustainment routes, and improving positional depth in the southern theatre.

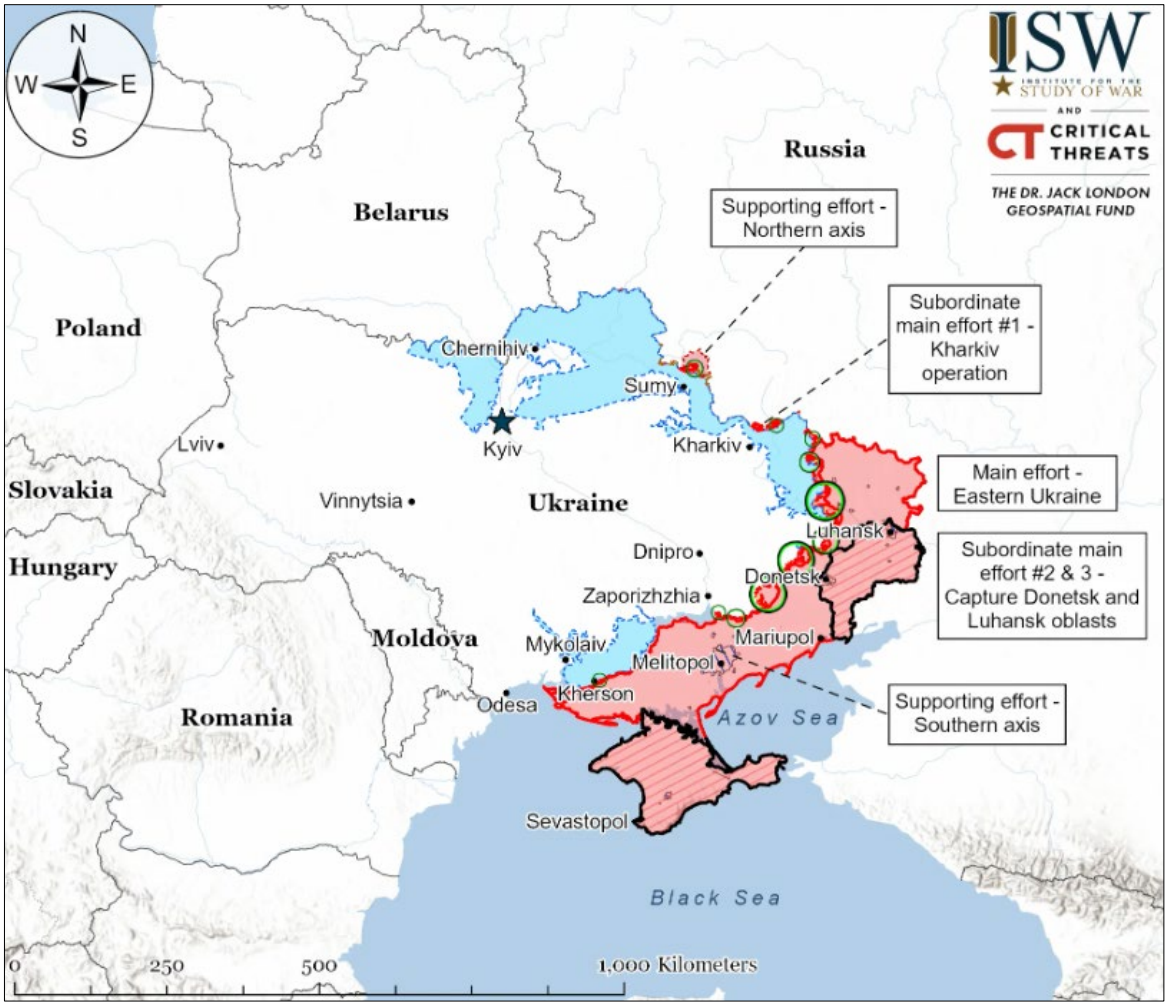

Figure 6: Assessed Control of Terrain in November 2025 (ISW 2025a)

At the strategic-political level, Russian declaratory policy increasingly reflected maximalist intent, as evidenced by official statements and public dissemination of operational mapping indicating potential objectives beyond currently occupied territories, including the Sumy, Kharkiv, Dnipropetrovsk, Mykolaiv, and Odesa regions. These statements served both strategic signalling and information operations purposes, reinforcing long-term Russian objectives and shaping perceptions of escalation dominance.

Conversely, Ukrainian operational planning in 2025 indicated limited prospects for large-scale counter-offensive operations. The primary focus shifted towards holding existing defensive lines, preserving forces, and regenerating combat capability, with the expectation of future capability enhancement through continued Western military assistance, including potential airpower enablers. Operational experience from previous campaigns demonstrated that without substantial degradation of Russian defensive systems, the probability of achieving an operational breakthrough remained limited.

The operational environment was further influenced by seasonal factors. The onset of autumn and associated terrain degradation (*rasputitsa* conditions) reduced mobility for mechanised formations, constrained manoeuvre warfare, and favoured forces operating from prepared defensive positions integrated with obstacle systems and minefields. Under these conditions, Russian forces increasingly employed a hybrid defensive–offensive posture across multiple sectors.

In sum, autumn 2025 marked the consolidation of a protracted attritional phase characterised by sustained Russian operational initiative and Ukrainian efforts focused on defensive stabilisation. Both battlefield developments and strategic indicators suggest that, absent a significant shift in force ratios or external support dynamics, Ukraine will continue to face increasingly demanding conditions in maintaining defensive coherence across the theatre of operations.

1.10 Consolidation of the Attritional Operational Environment from Autumn 2025

The period from autumn 2025 to the beginning of 2026 was a critical phase in the conflict's overall development. As anticipated, the onset of adverse meteorological conditions significantly influenced the operational environment. Seasonal rainfall followed by winter weather phenomena reduced terrain trafficability, constrained the manoeuvre of mechanised formations, and contributed to a partial stabilisation of selected sectors along the frontline.

These conditions enabled Ukrainian forces to achieve limited short-term operational effects in terms of force reconstitution, unit regeneration, and partial reorganisation of defensive positions. However, Russian forces simultaneously exploited the same environmental constraints to consolidate previously gained territory, improve sustainment and logistical depth, and prepare conditions for subsequent offensive activity. A key element of the Russian operational approach remained the sustained execution of deep-strike operations against Ukrainian operational depth, with particular emphasis on critical infrastructure, including energy-generation systems, industrial capacity, and logistical nodes.

From a capability perspective, a defining feature of this phase was the continued emphasis on firepower generation by both belligerents. Russian forces maintained a high tempo of long-range strike operations throughout the winter period, supported by sustained ammunition availability, ongoing production capacity, and external supply channels. This enabled Russia to maintain operational pressure both along the front line and within the Ukrainian rear area, thereby reinforcing the campaign's attritional character. Concurrently, the level, timing, and predictability of Western security assistance to Ukraine remained a decisive variable influencing Ukrainian force readiness, sustainment capacity, and operational flexibility.

In parallel, Ukrainian forces continued to conduct limited offensive operations through targeted strikes against Russian logistics nodes, command-and-control elements, and other high-value targets within operational depth. These activities, while tactically effective in selected instances, did not generate operational-level breakthrough effects. Nevertheless, they contributed to disrupting Russian planning cycles and imposed additional friction on sustainment and operational tempo. Despite these efforts, it was evident that without substantial qualitative reinforcement—particularly in the domains of combat aviation, ammunition supply, and force-generation capacity—Ukraine’s ability to transition back to large-scale offensive operations remained constrained.

Overall, this phase confirmed the continued Russian retention of the operational initiative. Russian forces consistently shaped the tempo and spatial distribution of operations, compelling Ukrainian forces to adopt a reactive and predominantly defensive posture. The principal Ukrainian operational objective remained the preservation of combat effectiveness, the retention of key defensive positions, and the prevention of operational breakthrough.

In retrospect, the autumn 2025–winter 2026 period did not produce a decisive strategic resolution. Instead, it reinforced the conflict's structural trajectory as a protracted war of attrition characterised by sustained Russian operational initiative. This phase further underscored that the ability to maintain initiative—understood as the capacity to dictate operational tempo and compel adversary reaction—remains a central determinant of effectiveness in contemporary high-intensity warfare.

2. TRANSITION TO ATTRITION WARFARE IN A MULTI-DOMAIN OPERATING ENVIRONMENT

What distinguishes the Russia–Ukraine War from most post-Cold War conflicts is the convergence of legacy military systems and emerging technologies within a high-intensity conventional warfare environment. The conflict has reaffirmed the enduring classic theory of war (Clausewitz 1989) while demonstrating the operational value of commercially available technologies, asymmetric capabilities, and large-scale force generation. It has also highlighted the growing importance of the moral component of fighting power, including societal resilience, strategic communications, information activities, and international coalition support, all of which help shape the operational environment, mitigate threats, exploit opportunities, and influence strategic outcomes.

The conflict provides a valuable case study of the ongoing transition from Allied joint operations towards MDO. Although an integrated NATO multi-domain concept has not yet been fully achieved, the war demonstrates the increasing convergence of capabilities and effects across the land, air, maritime, cyber and space domains. This transition remains constrained by the continued reliance on legacy platforms, force structures, and doctrinal concepts developed for earlier forms of warfare, which are not fully optimised for the requirements of contemporary multi-domain operations.

Both Russia and Ukraine have undertaken force adaptation measures intended to improve integration across domains and enhance operational effectiveness. However, the ability to transform military organisations remains heavily influenced by industrial capacity, economic resilience, and the ability to sustain prolonged combat operations. The demands of a wartime economy require the allocation of substantial national resources to force generation, force sustainment, equipment maintenance, ammunition production, personnel replacement, and the regeneration of combat power. In a protracted conflict, these factors become critical determinants of operational endurance. In this regard, Russia continues to benefit from greater demographic, industrial, and economic capacity, enabling it to absorb losses and sustain military operations over an extended period.

The conflict demonstrates that military doctrines are evolving in response to changing operational realities. Combat experience remains the ultimate mechanism for validating, refining, or disproving doctrinal assumptions and operational concepts. Consequently, both armed forces are actively adapting their organisations, tactics, techniques, and procedures (TTPs) to establish conditions favourable to future operational success. From a doctrinal perspective, Multi-Domain Operations represent the logical evolution of joint and combined-arms warfare. This approach seeks to integrate technological innovation with emerging operational concepts to achieve synchronised effects across all domains.

Future armed forces will increasingly need to master capabilities such as cyber operations, electromagnetic spectrum operations (EMSO), artificial intelligence-enabled decision support, autonomous systems, and accelerated command-and-control processes. The ability to generate decision advantage, maintain freedom of action, and impose multiple dilemmas on an adversary will be essential for both effective deterrence and success in high-intensity conflict. In this context, the Russia–Ukraine War may ultimately be viewed as a pivotal stage in the broader transition toward a fully integrated multi-domain battlespace.

2.1 Historical Parallel to Attritional Phase of the Russia–Ukraine War

Historical experience demonstrates that major transformations in warfare rarely occur abruptly. While each conflict retains its own strategic, political, and operational specificities, developments in military technology, doctrine, and operational art tend to evolve cumulatively. Armed conflicts, therefore, often expose and accelerate pre-existing trends rather than generating entirely new forms of warfare.

The First World War provides a useful historical analogy. The emergence of operational stalemate and large-scale attritional warfare resulted not only from mass mobilisation but also from a significant increase in tactical lethality. Advances in artillery, machine guns, and defensive field fortifications substantially enhanced defensive combat power and reduced the effectiveness of traditional offensive manoeuvres. Although these trends had already been observable in several late nineteenth-century conflicts, many European military establishments failed to fully integrate their implications into doctrine and operational planning prior to 1914.

Conversely, the final phase of the First World War demonstrated how the introduction of new operational concepts could restore manoeuvre to the battlefield. The integration of armoured formations, air power, infiltration tactics, and combined-arms operations enabled forces to achieve operational penetration and generate effects beyond the tactical level. While these developments influenced interwar military thought, adaptation was uneven across armed forces, with some retaining incremental doctrinal evolution rather than undertaking comprehensive transformation—often with significant consequences when confronted by more adaptive adversaries.

Analytical studies indicate that major changes in warfare emerge from the interaction between technology, doctrine, and operational adaptation (Chevassus 2025). One of the most significant lessons of the Russia–Ukraine War is the renewed centrality of attrition warfare, which has become the dominant operational logic of the conflict and warrants structured analytical separation.

In general terms, attrition warfare may be understood as comprising two interrelated phases. The first phase extends from the onset of hostilities until one side achieves a relative or decisive advantage over its adversary. This phase may persist for years and is characterised by the mobilisation of national human and material resources, particularly in existential conflicts, as well as by the stabilisation or consolidation of the frontline following initial manoeuvre operations.

During this phase, combat operations are dominated by indirect fire engagements, limited offensive actions at the tactical and local levels, and sustained deep strikes using air and missile capabilities against critical infrastructure and high-value targets that are difficult to repair or to replace rapidly. The primary operational objective is the systematic degradation of the adversary’s combat capabilities and force regeneration potential over time.

Degradation efforts are typically accompanied by limited, locally focused offensive actions aimed at improving tactical posture and seizing advantageous terrain along the line of contact. Large-scale offensive operations are generally constrained, as they are likely to encounter dense, layered defensive systems—characterised by extensive minefields, fortified positions, and sustained indirect fires—resulting in disproportionate expenditure of personnel and materiel.

In this context, even tactically successful deep offensive manoeuvres in the initial phase may yield only limited operational or strategic effect, particularly if the terrain gained does not translate into a corresponding reduction in the adversary's combat power or regeneration capacity.

The second phase of an attritional conflict emerges when one belligerent achieves sustained superiority in air power, long-range fires, and Intelligence, Surveillance and Reconnaissance (ISR), while simultaneously degrading the adversary’s force structure and regeneration capacity to the extent that it can no longer effectively replace losses, conduct force rotation, or reinforce threatened sectors. Under these conditions, the superior force can conduct successive limited-objective offensive operations across a broad frontage, supported by an integrated air defence and fires architecture. The operational purpose of this phase is the progressive exhaustion of the adversary’s remaining combat power, the disruption of command-and-control cohesion, and the degradation of morale, ultimately generating localised breakdowns of defensive integrity. Once a breach is achieved in a selected sector, these effects may cascade across the wider theatre, enabling exploitation operations and subsequent deep strikes against operational and strategic targets within adversary territory.

2.2 Collateral Aspects of Attritional War

In attritional warfare, the economic and industrial dimension is decisive. The defence industrial base, supported by resilient logistics networks and critical infrastructure, must be capable of sustaining the large-scale production of combat platforms, ammunition, military equipment, and spare parts required for both force expansion and enduring prolonged high-intensity combat operations. Industrial capacity must simultaneously support force regeneration and the generation of new combat formations.

Sustaining a war of attrition cannot rely exclusively on the production of technologically advanced weapon systems. Although such systems provide superior battlefield effectiveness, they are costly, time-intensive to manufacture, and require highly trained operators. Consequently, they cannot alone satisfy the requirements of a protracted, resource-intensive conflict. A balanced procurement and production approach is therefore required, combining advanced precision capabilities with large-scale production of simpler, robust and rapidly deployable systems. Given operational demand and economic constraints, mass production naturally focuses on the latter category, enabling the rapid training, equipping and deployment of mobilised personnel, as well as the replenishment of forces already engaged in combat operations. Nevertheless, advanced weapon systems remain indispensable for conducting precision strikes against high-value operational and strategic targets in the adversary's depth (Vershinin 2024).

2.3 Strategic Endurance and Defence-Industry Mobilisation

Having clarified the nature and objectives of attritional warfare, it is possible to apply these theoretical concepts to the Russia–Ukraine conflict in 2025. After nearly four years of high-intensity combat operations, the conflict has evolved into a predominantly force-oriented war of attrition. Given its existential significance for both the Ukrainian state and the Russian political leadership, the conflict has been characterised by the progressive mobilisation of military, economic, industrial and societal resources, accompanied by sustained external and internal support mechanisms.

The ongoing conflict can be assessed as remaining within the initial phase of attritional warfare. The operational environment is characterised by a relatively stable and heavily fortified front line, while force generation and resource mobilisation efforts continue on both sides. Offensive operations remain limited in depth, gradual in tempo and predominantly tactical in nature. Neither belligerent has achieved the level of operational superiority required to conduct a decisive, large-scale offensive capable of producing strategic breakthrough effects.

A defining characteristic of the Russia–Ukraine war is the critical importance of the time factor. Temporal dynamics significantly influence all domains of the conflict, including force mobilisation, defence-industrial production, economic sustainability, and societal resilience on the home front. Several factors contribute to the protracted nature of the war. Most notably, the absence of decisive air superiority, combined with sustained support from external actors through industrial production, financial assistance, intelligence sharing, and other strategic enablers beyond the direct reach of military destruction, has enhanced the endurance and resilience of both sides.

From an economic perspective, both Russia and Ukraine continue to allocate substantial and increasingly large national resources to sustain long-term warfighting requirements. In particular, the Russian state budget for 2025 reflects the continued prioritisation of defence expenditure and military production in support of ongoing operations. The Stockholm International Peace Research Institute (SIPRI) estimates that in 2025 the share of GDP allocated to defence will be 7.2% (about 15.5 trillion roubles, or about $183.2 billion based on the average real exchange rate for 2025, which is an 84.6% increase compared to 37.6 roubles per dollar), the previous year (Cooper 2025).

Table 3: Military expenditure of the Russian Federation in real terms, 2015–27 (Cooper 2025)

	GDP			Military expenditure		
Year	Total (m. roubles)	Change (%)	GDP deflator	Total (m. roubles)	Change (%)	As share of GDP (%)
2027[a]	248 313 000	*+2.8*	104.7	15 160 627	*–2.3*	*6.1*
2026[a]	230 568 000	*+2.6*	104.7	14 815 144	*–8.4*	*6.4*
2025[a]	214 575 000	*+2.5*	106.8	15 453 678	*+3.4*	*7.2*
2024	200 039 500	*+4.1*	108.9	14 000 000[b]	*+53.0*	*7.0*
2023	176 413 900	*+4.1*	108.0	8 400 000[b]	*+17.0*	*4.8*
2022	156 941 000	*–1.4*	118.2	6 648 000[b]	*+15.8*	*4.2*
2021	134 727 500	*+5.9*	118.2	4 859 035	*–5.2*	*3.6*
2020	107 658 100	*–2.7*	100.9	4 335 251	*+2.1*	*4.0*
2019	109 608 300	*+2.2*	103.3	4 209 409	*+3.7*	*3.8*
2018	103 861 700	*+2.8*	110.0	3 928 147	*–3.6*	*3.8*
2017	91 843 154	*+1.8*	105.3	3 704 422[c]	*–8.2*	*4.0*
2016	85 616 100	*+0.2*	102.8	3 830 548[c]	*–7.5*	*4.5*
2015	83 087 400	*–2.0*	107.2	4 026 284	*+16.5*	*4.8*

Russian budgetary planning, particularly since the beginning of military operations, has been characterised by limited transparency and the presence of concealed or non-attributable expenditure categories. Consequently, actual defence-related spending is assessed to be significantly higher than officially declared figures.

In contrast, estimates of Ukrainian military expenditure are provided, inter alia, through assessments published by the Organisation for Economic Co-operation and Development (OECD; OECD 2025). Based on this data, Ukrainian defence expenditure has increased since 2022, exceeding 20% of GDP and projected to reach approximately 26% in 2025, while an additional 18% of GDP is accounted for by external economic and financial assistance. Within the context of protracted attritional warfare, defence-industrial capacity is a decisive factor in sustaining combat operations and generating long-term military effectiveness. Although Ukraine inherited a substantial heavy industrial base from the former Soviet Union, a significant portion of this capacity declined after the USSR's dissolution. Consequently, at the outset of the conflict, Ukraine's defence industrial and manufacturing sectors were insufficiently prepared to sustain the requirements of a large-scale, long-duration war of attrition.

The provision of advanced weapon systems and cutting-edge technologies, including Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities, as well as satellite-based intelligence assets, remains largely dependent on support from Western Allies, as Ukraine currently lacks the technological base, industrial capacity and resources required for their autonomous development and production. These offensive and defensive capabilities are essential for protecting critical infrastructure and key assets, as well as for engaging and neutralising adversary targets. Existing shortfalls in the domestic production of advanced military equipment are partially mitigated by extensive national efforts and significant internal reforms. High-level military authorities should serve as facilitators—removing barriers, securing funding, and ensuring interoperability—while enabling lower-level commands to identify and adopt urgently needed technologies. Ukraine's experience illustrates how interagency (or interservice) collaboration, combined with strategic prioritisation of technology deployment and resource allocation, can streamline innovation by removing bureaucratic barriers (Bondar 2025).

In 2024-2025, the war openly becomes a race between Ukrainian exhaustion and Western weariness—the temporal gamble of Russian attrition. These temporal principles—transforming duration into a strategic advantage, exploiting favourable asymmetries, betting on the adversary's exhaustion—shed light on contemporary Russian conduct in Ukraine, where the same logic operates in a radically different technological context.

3. KEY FACTORS OF THE MULTI-DOMAIN OPERATING ENVIRONMENT IN UKRAINE

The conflict demonstrates that contemporary military operations can no longer be analysed within the confines of individual domains. Instead, operational success increasingly depends on the ability to integrate and synchronise effects across the land, air, maritime, cyber and space domains. Nevertheless, the character of the conflict has evolved differently within each domain, reflecting distinct operational challenges and opportunities.

In the land domain, the conflict has progressively evolved into a war of attrition, characterised by intensive indirect fires, extensive defensive fortifications, high personnel and materiel losses, and sustained competition in force generation, force sustainment, and defence-industrial capacity. In the air domain, neither belligerent has succeeded in establishing enduring air superiority, resulting in a highly contested air environment in which integrated air and missile defence (IAMD) systems, EMSO, and long-range precision fires have significantly constrained freedom of manoeuvre and operational reach.

In the maritime domain, particularly within the Black Sea theatre, the extensive employment of long-range precision strike capabilities and uncrewed maritime systems has challenged traditional concepts of sea control and maritime power projection. These developments have demonstrated the increasing vulnerability of naval forces operating within contested maritime environments characterised by persistent surveillance and precision targeting.

The cyber domain has emerged as a fully integrated operational domain, supporting both offensive and defensive cyber operations targeting military networks, critical infrastructure, command-and-control systems, and information environments. The conflict has further highlighted the importance of resilience and cybersecurity as essential components of national and military defence.

Beyond the above domains, the war has underscored the growing significance of the cognitive dimension of warfare. Information and psychological operations have become critical instruments for maintaining societal resilience, influencing perceptions, shaping decision-making processes, and sustaining domestic and international political support. Collectively, these factors have significantly influenced the Russia–Ukraine War to shape the contemporary multi-domain operating environment.

3.1 Land Domain - Attrition as Dominant Factor

A defining characteristic of the current phase of the conflict, particularly in the land domain, is its evolution into a war of attrition. As of February 2026, the conflict has entered its fifth year without either belligerent achieving a decisive strategic outcome. However, this apparent operational stalemate conceals an important strategic dynamic. Since late 2023, Russian forces have pursued a systematic attritional approach aimed at degrading Ukrainian military capabilities through sustained operational pressure, incremental territorial gains, and the continuous depletion of Ukrainian personnel, equipment, ammunition, and other critical resources.

In essence, attrition warfare does not prioritise rapid operational decision but instead focuses on the systematic degradation of the adversary's combat potential while preserving one's own force effectiveness. The outcome is determined less by single decisive manoeuvres and more by cumulative exhaustion of personnel, materiel, and industrial capacity over time. This approach has been applied in the gradual seizure of terrain in key sectors of the Donbas operational area, including the battles for Bakhmut, Avdiivka, Vuhledar, and Pokrovsk; sustained long-range strikes against critical infrastructure and military-support facilities; and persistent offensive activity across a front extending approximately 1,200 kilometres. At the same time, several major Russian urban and operational engagements—including Mariupol, Bakhmut, and Avdiivka—have reflected sustained efforts to overcome and dismantle the resilience of Ukrainian defensive formations.

However, allocating substantial combat power to the defence of politically or symbolically significant objectives introduces operational risk. In certain circumstances, political and moral imperatives may outweigh strictly military considerations, potentially leading to disproportionate expenditure of personnel, equipment, and ammunition. Over time, such dynamics may reduce overall force effectiveness and affect the coherence and sustainability of defensive operations across the wider theatre.

Rather than seeking a rapid breakthrough or decisive operational manoeuvre, Russian strategy has increasingly focused on exhausting Ukrainian combat power, undermining force regeneration, and exploiting advantages in manpower, industrial output, and strategic depth to achieve cumulative operational and strategic effects over time. Another significant aspect of the current phase of the conflict is that the war has accelerated the emergence of an operating environment characterised by unprecedented battlefield transparency.

The widespread availability of space-based, airborne and terrestrial sensors, combined with advanced ISR capabilities, has significantly reduced the ability of forces to conceal, camouflage and mass combat power without detection. Intelligence support provided to Ukraine by Western partners, especially the United States, has enabled near-continuous monitoring of Russian force movements, force concentrations and logistical activities.

Within this environment, autonomous systems have become indispensable operational tools. Employed across all echelons and domains, they function simultaneously as reconnaissance platforms, targeting assets and precision-strike systems. Their relatively low cost, rapid production cycles and operational flexibility enable persistent surveillance and engagement of targets throughout the tactical battlespace and, increasingly, within the operational depth.

The conflict has also demonstrated the decisive importance of Electronic Warfare (EW). Both belligerents employ EW capabilities to disrupt C2 systems, degrade communications, interfere with navigation signals and reduce the effectiveness of unmanned systems. The integration of EW capabilities with extensive UAS employment has significantly shortened the sensor-to-shooter cycle, enhanced target acquisition and improved the effectiveness of precision fires. In several sectors, these capabilities have enabled Russian forces to achieve local tactical advantages despite broader operational constraints.

At the same time, some analysts caution against treating the Russia–Ukraine war as a universally applicable model of future conflict (Gris 2025). They argue that many observed phenomena are shaped by specific contextual factors, including the geographical characteristics of the theatre, the relative balance of military capabilities, the extensive involvement of external actors, and the distinct political and strategic objectives of the belligerents. From this perspective, the conflict should be viewed not as a universally representative model, but rather as an extreme—albeit highly instructive—case study of contemporary warfare.

Many analysts assess that one of the key strategic consequences of the initial Russian operational concept in February 2022—based on assumptions consistent with rapid manoeuvre and decisive operational shock—was the failure to achieve strategic decision through a short-duration campaign. This outcome contributed to an adaptation in Russian strategic behaviour, culminating in the transition toward a protracted war of attrition, characterised by sustained pressure, cumulative losses, and incremental territorial gains.

As noted in analytical studies (Vershinin 2024), it is essential to distinguish attrition warfare from the manoeuvre warfare concept traditionally preferred by many Western armed forces. Manoeuvre warfare is primarily terrain- and decision-centric, seeking rapid dislocation of enemy forces and achievement of strategic objectives through speed, concentration of effects, and operational surprise, typically enabled by highly professional force structures. In contrast, attrition warfare is fundamentally force-centric, in which the decisive variables are industrial capacity, depth of manpower reserves, the ability to regenerate combat power, and the availability of time to sustain prolonged operations.

The conduct of military operations in the Russia–Ukraine conflict demonstrates the defining characteristics of modern attritional warfare and differs fundamentally from classical manoeuvre warfare. Rather than pursuing rapid operational breakthroughs alone, both belligerents increasingly focus on the systematic degradation of the opponent's combat power, logistics network, defence industrial capacity and force regeneration potential, while simultaneously preserving their own operational endurance.

The battlefield in Ukraine is heavily saturated with interconnected reconnaissance and strike capabilities, including UAS, long-range precision fires, EW assets, artillery, loitering munitions and integrated reconnaissance-strike complexes. Under such conditions, the large-scale concentration of personnel and armoured formations required for deep manoeuvre operations entails extremely high risk due to continuous exposure to ISR-enabled targeting, massed indirect fires and precision strikes. This reality has significantly reduced the feasibility of large-scale operational manoeuvres without first degrading the adversary's reconnaissance and fire-support architecture.

Both Russian and Ukrainian forces therefore operate within layered defensive frameworks that integrate air defence systems, EW assets, counter-battery capabilities, and UAS-supported ISR networks. The establishment of such a protective "bubble" is essential for the survivability of forces engaged in both defensive and offensive operations. Ukrainian offensive operations conducted in 2023 demonstrated the extreme complexity of breaching prepared defensive belts protected by dense minefields, layered artillery coverage, attack drones and integrated fire-control systems. Insufficient coordination among reconnaissance assets, EW support, engineering units, artillery fires, and manoeuvre formations significantly increases attrition before assault units can even reach primary defensive positions.

Consequently, offensive operations in Ukraine are generally limited to advances conducted within the effective range of supporting air defence, EW and fire-support systems. Any deeper penetration requires the continuous forward displacement of these protective layers to preserve freedom of manoeuvre for advancing units. Such operations place considerable demands on command and control, logistics and operational synchronisation. In contrast, semi-static frontlines — characteristic of large sectors of the conflict — are easier to sustain and manage, particularly when forces include rapidly mobilised personnel with varying levels of training and combat experience.

The conflict has also highlighted that success in attritional warfare depends heavily on industrial and economic resilience. Both sides seek to degrade the opponent's force regeneration capability through long-range strikes against ammunition depots, fuel storage facilities, transportation infrastructure, defence-industrial sites and energy networks. Russian strikes against Ukrainian energy infrastructure and Ukrainian long-range attacks against Russian oil refineries, logistics hubs and military-industrial facilities illustrate this mutual strategy of strategic attrition. Priority targets are generally infrastructure and production capacities that are difficult, resource-intensive or time-consuming to repair or replace, thereby generating cumulative long-term operational effects.

The war in Ukraine further demonstrates that, in the absence of decisive air superiority, the degradation of an adversary's military and industrial capabilities becomes a prolonged process. Both belligerents possess substantial integrated air defence capabilities, extensive use of camouflage, concealment and deception measures, and increasingly dispersed logistics and production networks. Consequently, neither side has been able to achieve the level of operational freedom traditionally associated with uncontested air dominance, contributing to the conflict's prolonged, highly attritional character.

3.2 Air Domain - Air Superiority Principle and the Russia–Ukraine War

Another important aspect of the Russia–Ukraine war is that neither side has air superiority, either overall or regional. Mobile and layered air defences, along with various electronic warfare systems, disrupt ground offensive operations and the use of guided munitions, thereby emphasising the role of unmanned systems, democratising traditional forms of aviation and conventional artillery, and making it difficult for infantry to move.

3.2.1 Changing Character of Contemporary Air Operations

The lack of air superiority facilitated the initial resistance and the transition from a war of movement to a war of attrition (Slusher 2025). Within NATO doctrine, air power is the capability to generate military effects and influence adversaries' behaviour by employing air and space capabilities across the full spectrum of military operations. The enduring relevance of air power stems from its ability to provide freedom of action, situational awareness, rapid force projection, and precision engagement across the tactical, operational, and strategic levels of warfare.

Historically, control of the air has been a decisive factor in major conflicts. From the Second World War to more recent campaigns, the ability to achieve and exploit air superiority has enabled military forces to protect friendly forces, disrupt adversary operations, and conduct sustained offensive action across all domains. Air superiority facilitates freedom of manoeuvre for land, maritime, and air forces while simultaneously restricting the adversary's ability to employ its own capabilities effectively (Biddle 2006).

The Russia–Ukraine War, however, illustrates both the enduring importance of air power and the challenges associated with achieving it against a capable opponent. Unlike many post-Cold War conflicts, neither Russia nor Ukraine has been able to establish comprehensive air superiority over the theatre of operations. Instead, both sides operate in a highly contested air environment characterised by dense, layered IAMD, extensive EW use, and persistent ISR coverage.

As a result, the conflict has demonstrated that the ability to project combat power from the air remains essential, but its employment is increasingly constrained by modern air-defence networks and the proliferation of long-range precision-strike capabilities. Air operations are therefore conducted under significant risk, thereby limiting the freedom of action traditionally associated with uncontested air superiority. This reality has contributed to the growing importance of stand-off weapons, UAS, electronic warfare capabilities, and space-enabled ISR support as means of generating operational effects without exposing high-value aircraft to unacceptable levels of risk.

From a NATO perspective, the conflict reaffirms that credible deterrence and effective military operations require not only advanced air power capabilities but also the ability to integrate them into a coherent joint campaign. Achieving operational objectives depends on the synchronised employment of air, land, maritime, cyber, and space capabilities to support clearly defined military and political end-states.

The ability to establish at least localised and temporary air superiority, suppress or degrade adversary air-defence systems, and maintain freedom of action within the electromagnetic spectrum remains a fundamental prerequisite for successful large-scale operations.

The war also highlights the extraordinary versatility of air power. Air and space capabilities can rapidly transition between missions, including air superiority, ISR, strike operations, close air support, air mobility, strategic transport, airborne command and control, suppression of enemy air defences (SEAD), destruction of enemy air defences (DEAD), and missile defence. This flexibility enables commanders to respond rapidly to changing operational requirements and generate effects across multiple domains simultaneously.

At the same time, the Russia–Ukraine conflict demonstrates that air power is no longer limited to manned aviation. The increasing integration of UAS, long-range precision weapons, commercial and military satellites, electronic warfare systems, and advanced command-and-control networks is transforming the character of air operations. Future air campaigns are therefore likely to depend less on the exclusive use of traditional combat aircraft and more on integrating manned and unmanned systems within a multi-domain operational framework capable of generating sustained effects across the entire battlespace.

3.2.2 Air Superiority and Operational Effectiveness in Ukraine

The Russia–Ukraine War has reaffirmed the central role of air power in contemporary warfare while simultaneously demonstrating the challenges of employing it in a highly contested operational environment. Air capabilities contribute across the full spectrum of military operations, including ISR, tactical and strategic air mobility, special operations support, precision strike missions, IAMD, Personnel Recovery (PR), EW, Airborne Early Warning and Control (AEW&C), Suppression and Destruction of Enemy Air Defences (SEAD/DEAD), and the employment of UAS. The conflict in Ukraine provides numerous examples of each of these functions and highlights their growing interdependence within a multi-domain battlespace.

From a doctrinal perspective, military success is generally facilitated by the ability to establish and exploit air superiority. Nevertheless, the Russian Air Force failed to establish sustained air superiority over Ukraine, a prerequisite that many Western analysts had considered essential for the rapid achievement of Russian operational objectives. Control of the air enables freedom of action across all domains, protects friendly forces from air attack, enhances operational mobility, and permits the effective application of fires against adversary forces and critical vulnerabilities.

Consequently, a state possessing superior air capabilities would traditionally be expected to enjoy a significant operational advantage over an opponent (Nesselhuf 2025).

The Russia–Ukraine War, however, demonstrates that numerical and technological superiority in air assets does not automatically translate into air superiority or strategic success. At the outset of the conflict, Russia possessed a substantial quantitative and qualitative advantage in combat aviation, long-range strike systems, and air capabilities.

Several factors contributed to this outcome. Ukraine maintained a resilient and adaptive IAMD network, supported by dispersed operations, effective camouflage and deception measures, mobile air-defence systems, and increasing assistance from Western partners. In parallel, both sides employed extensive electronic warfare capabilities, while the proliferation of Unmanned Aerial Vehicles (UAVs) and the availability of near-persistent ISR coverage increased the transparency of the battlespace and complicated the conduct of air operations. As a result, Russian airpower has been unable to operate with the degree of freedom traditionally associated with modern air campaigns conducted by NATO forces.

The conflict, therefore, illustrates a critical distinction between possessing significant airpower resources and being able to translate those resources into effective operational outcomes. Although Russia has achieved localised and temporary air superiority in specific sectors, it has been unable to establish theatre-wide air superiority or air supremacy. This limitation has constrained its ability to conduct deep manoeuvre operations, provide persistent close air support, interdict Ukrainian logistics at scale, and achieve decisive operational effects through air power alone.

The UAV empowers the Russian army and takes pressure off the Russian Air Force to evolve. The Russian army prefers UAVs and ground-based air defence, which it can control and that do not require contentious coordination with other services. Russia's new ground manoeuvre system will build on the UAV as its air-support and reconnaissance capability and attempt to free itself from the slower air system. The Russian Air Force, likewise, appears content to divest the close air support mission to focus on its primary defensive missions and standoff operations (Wiswesser 2023).

Ukraine has been conducting a coherent campaign to suppress and destroy Russian air defences since late 2024, shaping the battlefield as part of more sophisticated campaign planning. SEAD/DEAD refer to tasks to destroy or temporarily degrade surface-based enemy air defences by destructive or disruptive means to let friendly aircraft operate safely.

Ukraine's degradation of the Russian air defence network through concentrated strikes against radars and air defence systems allows subsequent Ukrainian strikes to target other valuable assets in the Russian rear, enhancing the reach of Ukraine's mid-range strike campaign, enabling Ukrainian forces to launch a higher volume of drones and larger drones deeper into airspace over Russian-controlled terrain (ISW 2026b).

At the same time, the war highlights the continued relevance of Western airpower doctrine. NATO operational concepts emphasise the integration of air capabilities into a coherent joint campaign designed to achieve clearly defined political and military objectives. Such campaigns rely not only on advanced platforms but also on effective C2, ISR integration, SEAD/DEAD operations, precision targeting, logistics, training, and joint force synchronisation. The conflict suggests that the absence of these enabling factors can significantly reduce the effectiveness of even a numerically superior air force.

Figure 7: Ukraine's Strike Campaign Against Russian Counter-Air and Counter-Drone Defenses (ISW 2026b)

The Russia–Ukraine War should therefore not be interpreted as evidence that airpower has lost its importance. Rather, it demonstrates that achieving and maintaining air superiority against a capable and well-supported adversary has become considerably more complex. Future conflicts are likely to require integrating manned aircraft, UAS, long-range precision fires, cyber capabilities, electronic warfare, space-based assets, and advanced air-defence systems within a comprehensive multi-domain framework. In this environment, the ability to generate air effects remains indispensable, but success increasingly depends on integrating capabilities across domains rather than on employing airpower in isolation.

3.2.3 Command and Control System and the Use of Airpower

Another important factor highlighted by the Russia–Ukraine War concerns the employment of airpower and the organisation of C2. The conflict has demonstrated that the effectiveness of airpower is significantly influenced not only by the quantity and quality of available platforms but also by the way air capabilities are integrated into the joint force and employed within a coherent operational framework.

One of the persistent challenges observed in Russian operations has been the apparent fragmentation of airpower employment across multiple operational sectors. Air assets have frequently been allocated to support geographically defined ground-force groupings, resulting in a decentralised approach that appears to prioritise local tactical requirements over theatre-wide operational objectives. Such an approach can limit the flexibility of airpower and reduce the ability to concentrate effects at decisive points and times across the theatre.

From a NATO doctrinal perspective, the effective employment of airpower is based on the principle of centralised control and decentralised execution. This principle enables the commander responsible for the air component—typically the Joint Force Air Component Commander (JFACC)—to allocate, prioritise, and reallocate air assets in accordance with the joint force commander's objectives. Centralised control facilitates the concentration of combat power, operational agility, and rapid adaptation of air operations to changing battlefield conditions, while avoiding the inefficient distribution of scarce high-value capabilities across multiple competing priorities.

The conflict in Ukraine suggests that excessive sectoral allocation of air assets can constrain operational flexibility and reduce the ability to exploit the inherent advantages of airpower, namely its speed, reach, versatility, and capacity to generate effects across the tactical, operational, and strategic levels simultaneously.

When air capabilities are employed primarily in support of local ground-force requirements, their broader operational and strategic potential may not be fully realised. The war has also highlighted differing approaches to the role of airpower in joint operations. Russian military practice has traditionally emphasised the close integration of aviation with ground operations, often employing air assets in support of land manoeuvre and fire support missions. While such missions remain essential components of air operations, the conflict has demonstrated the limitations of viewing airpower primarily as an extension of ground fires. Contemporary NATO doctrine recognises airpower as an operational and strategic instrument capable of generating independent effects throughout the depth of the battlespace, including against command-and-control networks, logistics systems, critical infrastructure, force-generation capabilities, and other strategic centres of gravity.

Several operational episodes illustrate the consequences of failing to fully integrate airpower into a broader joint campaign. Early Russian attempts to seize key objectives, including the operation against Hostomel Airport, revealed challenges in synchronising air, land, and special operations forces. More broadly, Russian forces have struggled to establish sustained air superiority, protect manoeuvre formations from Ukrainian strike capabilities, and prevent Ukrainian long-range attacks against military, economic, and strategic targets within Russian-controlled territory and, increasingly, within Russia itself.

More than four years into the conflict, neither belligerent has achieved comprehensive air superiority. However, Russia's inability to translate its numerical advantage in combat aviation into theatre-wide freedom of action highlights the critical importance of integrated command and control, effective SEAD/DEAD operations, robust ISR support, and the synchronisation of airpower with broader joint-force objectives.

For NATO, the conflict offers several important lessons. First, airpower should continue to be viewed as a strategic and operational capability rather than solely as a supporting arm for land operations. Second, the principle of centralised control and decentralised execution remains essential to maximising the effectiveness of scarce, high-value air assets in contested environments. Third, achieving air superiority against a capable adversary requires integrating aviation, long-range precision fires, electronic warfare, cyber capabilities, space-based support, and intelligence assets into a coherent multi-domain operational framework.

Finally, the war underscores the need for NATO members to continue adapting their force structures, operational concepts, and capability-development processes to the realities of high-intensity warfare.

Following decades of counterinsurgency and expeditionary operations conducted under conditions of uncontested or near-uncontested air superiority, the Alliance must prepare for conflicts characterised by contested airspace, dense air-defence networks, persistent ISR coverage, and rapid cycles of technological adaptation. The experience of Ukraine demonstrates that future success will depend not only on technological superiority but also on the ability to integrate and employ military capabilities effectively across all domains of warfare.

3.3 Maritime Domain - Transformation of Naval Warfare

Between 2024 and 2025, the war between Russia and Ukraine produced significant transformations not only on land and in the air but also in maritime space, demonstrating that traditional naval supremacy can be rapidly eroded by asymmetric, creative, and relatively low-cost means. The Russian fleet, perceived for decades as an essential instrument of force projection in the Black Sea, became, during the conflict, a vivid example of the vulnerability of large conventional structures to new forms of warfare (Popa 2025).

Although the maritime dimension of the Russia–Ukraine war has received less public attention than land operations, it has played a decisive role in shaping both the operational environment and the conflict's broader strategic trajectory. The Black Sea and the Sea of Azov have served as critical theatres influencing force projection, economic security, logistics, and the protection of maritime lines of communication. Control, or denial of control, in these waters has had direct implications not only for military operations but also for the global flow of commodities, particularly grain exports.

3.3.1 Evolution of the Maritime Balance in the Black Sea

At the outset of the conflict, the Russian Federation possessed clear maritime superiority. The Black Sea Fleet operated as a dominant regional force, capable of projecting power throughout the basin and supporting joint operations through long-range precision strikes, amphibious operations, and blockade. This initial advantage enabled Russia to impose significant operational pressure on Ukraine, including restrictions on maritime trade and threats to coastal regions. However, this dominance proved progressively unsustainable. Ukrainian forces, despite starting from a position of severe naval inferiority, implemented a sustained campaign of maritime interdiction and denial. Through a combination of missile strikes, sabotage operations, and unmanned attacks, Ukraine systematically degraded Russian naval capabilities.

After the heavy blows it suffered in 2023, the Russian fleet entered 2024 fragile and on the defensive. Ukraine did not stop its campaign, however, and the first months of 2024 brought spectacular new attacks that sank the last major ships Russia still relied on in the Black Sea (Popa 2025).

By 2024, the cumulative impact of these operations had significantly reduced the Russian Black Sea Fleet's operational freedom, forcing it into a more defensive posture and limiting its ability to operate in the central and western Black Sea.

By early 2025, the maritime balance of power had undergone a fundamental transformation. Russian surface ships could no longer operate with relative impunity across large portions of the theatre. Instead, naval activity became increasingly constrained to the eastern Black Sea and areas adjacent to Crimea and the Russian mainland. Waters near Ukraine, Romania, and Türkiye evolved into contested operational zones, where persistent threats from Ukrainian long-range strikes and targeting networks restricted manoeuvre and increased risk exposure.

The consequences of this shift extend beyond the military domain. The degradation of the Black Sea Fleet has significantly weakened Russia’s capacity to project maritime power and reduced its ability to secure critical economic interests. Maritime trade routes, port infrastructure, and logistics hubs have become increasingly vulnerable, while the termination of arrangements such as the Black Sea Grain Initiative has further destabilised the regional maritime security environment. Commercial shipping has effectively been integrated into the broader strategic competition, illustrating the expanding scope of modern maritime conflict.

3.3.2 Integrated Maritime A2/AD

A central feature of the Black Sea campaign has been the emergence of a highly integrated maritime anti-access/area denial (A2/AD) construct, driven by the convergence of several technological and operational developments. As illustrated in Figure 8, these developments include persistent ISR, long-range precision-strike capabilities, and the integration of effects across multiple operational domains. Collectively, these elements have generated a fundamentally new approach to maritime warfare, significantly diminishing the effectiveness and survivability of traditional surface fleets operating in contested environments. At the core of this transformation is the growing capability to maintain continuous situational awareness across the maritime battlespace. Advances in ISR—ranging from satellite reconnaissance to unmanned aerial systems and electronic surveillance—have enabled Ukrainian forces to detect, track, and target Russian naval assets with increasing accuracy and speed.

This persistent surveillance environment has compressed decision-making timelines and shortened the sensor-to-shooter cycle, allowing strikes to be executed with minimal delay. The operational consequences of such ISR integration are profound. Naval platforms operating within the range of adversary strike systems are no longer able to rely on concealment, mobility, or dispersion as primary survivability mechanisms. Instead, they exist within a transparent battlespace where detection is increasingly probable, and engagement timelines are significantly reduced. This erosion of traditional maritime advantages represents a structural shift in naval warfare, particularly in geographically constrained littoral regions.

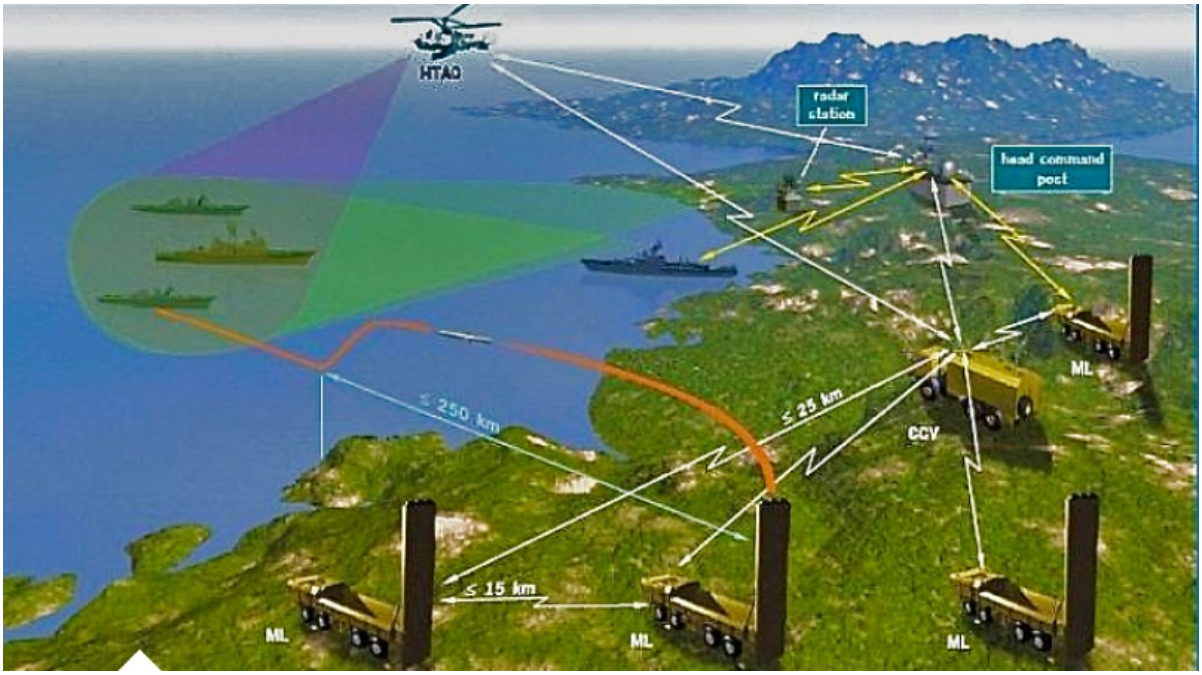

Figure 8: Russian Integrated Maritime A2/AD Strategy (Kofman 2020a)

Complementing this ISR architecture is the widespread use of precision-guided munitions. The Black Sea campaign demonstrates that the ability to generate significant maritime effects is no longer confined to naval forces alone. Land-based anti-ship missiles, air-delivered strike systems, and hybrid capabilities can achieve effectiveness levels comparable to those traditionally associated with surface combatants. When integrated into a networked targeting system, these capabilities enable a distributed approach to maritime warfare in which effects are generated across domains rather than concentrated within naval platforms. This convergence of ISR and precision strike has redefined the relationship between sea control and sea denial. Instead of relying on fleet engagements to secure dominance, Ukraine has employed a strategy focused on denying the adversary's ability to operate effectively within the theatre. This approach leverages cross-domain integration to compensate for conventional naval limitations, illustrating how smaller or less-equipped actors can challenge more powerful maritime forces through technological and operational innovation.

3.3.3 Uncrewed Systems and Asymmetric Naval Warfare

Within this integrated framework, uncrewed systems have emerged as one of the most transformative elements of the Black Sea campaign. The extensive use of Uncrewed Surface Vessels (USVs) and UAS has demonstrated their capacity to operate as both independent strike platforms and enablers of broader operational effects.

While the concept of unmanned maritime systems predates the conflict, their deployment in the Black Sea has reached an unprecedented level of operational maturity. Ukrainian forces have employed USVs not only as one-way attack platforms but also as modular systems capable of carrying a range of payloads, including ISR sensors, explosive charges, and auxiliary mission equipment. This adaptability has allowed them to perform a wide range of functions, from reconnaissance and targeting to direct engagement and disruption of naval operations.

The significance of these systems extends beyond their technical capabilities. Their relatively low cost, operational flexibility, and scalability make them particularly well-suited for asymmetric warfare. USVs can be deployed in large numbers, operate in contested environments with minimal risk to personnel, and impose disproportionate pressure on high-value naval assets. This creates a strategic dilemma for conventional navies, which must allocate significant resources to counter threats from comparatively inexpensive systems.

The cost-exchange dynamic observed in the Black Sea is especially noteworthy. Platforms valued at hundreds of millions of dollars have been damaged or neutralised by systems costing a fraction of that amount. This inversion of traditional cost structures challenges established procurement models and raises important questions about the future composition of naval forces. It suggests that effectiveness in modern maritime warfare may depend less on acquiring increasingly sophisticated platforms and more on integrating affordable, distributed capabilities into a coherent operational framework. Moreover, the success of uncrewed systems has contributed to a shift in Russian naval behaviour. Faced with persistent threats, the Black Sea Fleet has increasingly adopted a “fleet-in-being” posture, limiting its exposure and relying on protected bases and defensive measures rather than actively contesting maritime space.

This outcome underscores the strategic impact of asymmetric approaches, which can achieve significant effects without requiring decisive engagements. Looking forward, it is highly likely that lessons from the Black Sea will be replicated in other theatres. Both state and non-state actors are expected to adopt similar approaches, combining uncrewed systems with precision strike and ISR integration to challenge more advanced maritime forces. This trend highlights the growing accessibility of advanced military capabilities and the increasing complexity of future maritime threat environments.

3.3.4 Strategic Implications of the Black Sea Campaign

Beyond the operational level, the maritime campaign in the Black Sea has important strategic and geopolitical implications. An analysis of the maritime operating environment, including the territorial waters of the Black Sea and the Azov Sea (see Figure 9), highlights several significant findings. Among the most consequential is the need to reassess prevailing assumptions regarding escalation dynamics. Ukrainian strikes against military targets in Crimea—long regarded as actions carrying a high risk of escalation—did not provoke the level of Russian retaliation that many observers had anticipated. This experience suggests that perceptions of escalation risk may, under certain circumstances, be exaggerated, resulting in self-imposed political or military constraints that unnecessarily limit strategic and operational freedom of action.

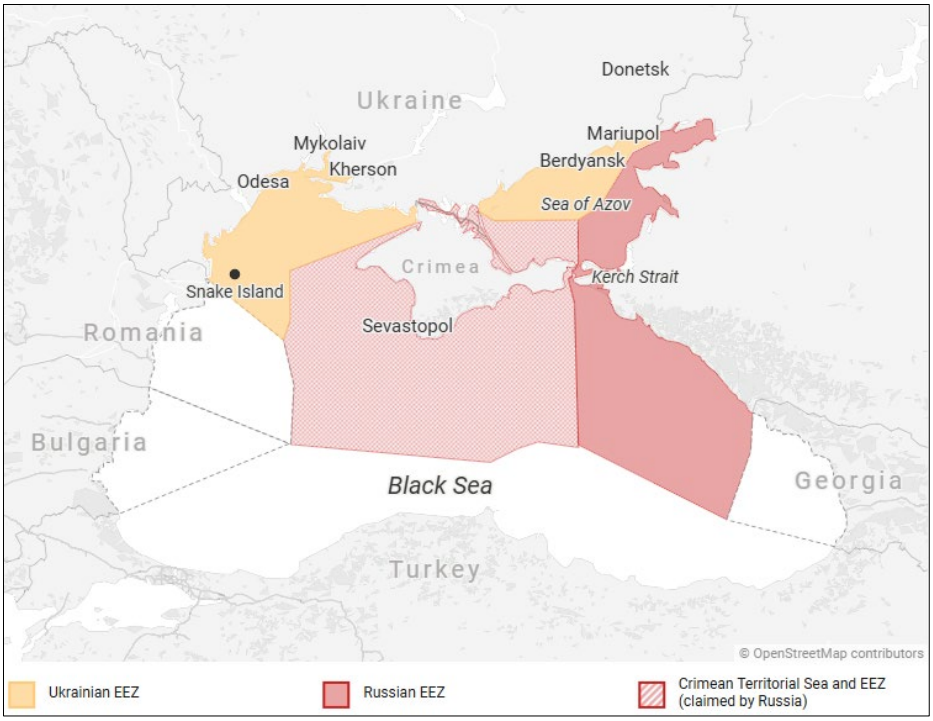

Figure 9: Russian maritime claims following the annexation of Crimea (CEPA 2018)

The implications extend beyond the Black Sea theatre. The conflict demonstrates how adversaries can leverage perceived escalation thresholds and deterrence narratives to influence decision-making, shape strategic behaviour, and constrain an opponent's options without necessarily possessing the intent or capability to execute the threatened response. Consequently, a more nuanced understanding of escalation management and deterrence is required. Reassessing these dynamics will be essential for future defence planning and crisis decision-making, particularly in conflicts involving nuclear-armed states, where the perceived risk of escalation can decisively influence political and military choices.

The conflict has also reaffirmed the importance of geography and control over maritime chokepoints. Türkiye's role as the gatekeeper of the Turkish Straits has given it significant influence over access to the Black Sea. By balancing its relationships with both Ukraine and Russia, Ankara has positioned itself as a key strategic actor capable of shaping regional security dynamics. This highlights the enduring relevance of geographic constraints and political factors in maritime operations.

At a broader level, the campaign demonstrates how modern maritime warfare extends beyond purely military considerations. Economic security, energy flows, and global trade are increasingly intertwined with military operations. The targeting of ports, logistics hubs, and commercial shipping reflects a shift toward comprehensive maritime competition, in which civilian and military domains are closely interconnected.

3.3.5 Paradigm of Modern Maritime Warfare

The cumulative effect of these developments' points to the emergence of a new paradigm of maritime warfare. The paradigm shift in maritime operations involves moving away from concentrating power in capital ships to distributing capabilities across a network of assets (Laird 2025). Traditional metrics of naval power—such as fleet size, tonnage, and platform capabilities—are becoming less decisive in an environment shaped by multi-domain integration, information dominance, and technological innovation. The Black Sea campaign illustrates that future maritime superiority will depend on the ability to integrate capabilities across domains and to operate effectively within highly contested environments. This includes the development of resilient command-and-control systems, enhanced force protection measures, and advanced countermeasures against unmanned and precision-strike threats (Kilinc 2026).

In October 2025, NATO published its revised Maritime Strategy, a political statement designed to deter adversaries while reassuring allied nations and their publics. Inevitably, commentators have paid significant attention to the contribution of the alliance's maritime elements to deter and defend member states' interests in the event of full-scale peer conflict. (Klein, 2025) Allies, through the commitment to NATO defence plans, shall take timely actions to maximise the warfighting readiness and effectiveness of current maritime forces while planning for the introduction of future capabilities. Fully resourced, agile, and flexible Standing Naval Forces (SNF) and NATO operations, missions, and activities are key to delivering maritime security in support of NATO's three core tasks. The SNF are a visible instrument of NATO's will to rapidly deter and defend across all domains.

For NATO and other maritime powers, these trends necessitate significant adaptation. Key areas for development (see Figure 10) include electromagnetic spectrum operations, cyber resilience, AI-enabled ISR, and distributed maritime operations. The ability to counter massed unmanned systems and maintain operational effectiveness under persistent surveillance will be a critical determinant of success.

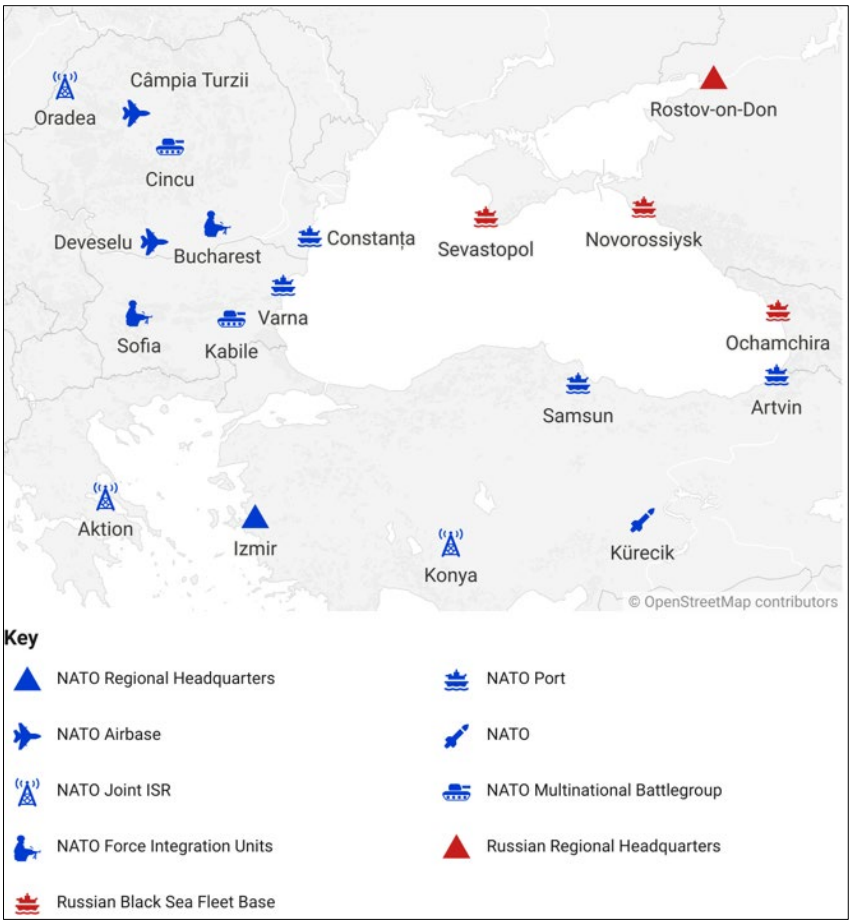

Figure 10: NATO and Russian military installations in the Black Sea area (Avdaliani 2023)

Importantly, the conflict also highlights the growing role of hybrid warfare in the maritime domain. Rather than large-scale fleet engagements, the Black Sea has witnessed a combination of conventional, asymmetric, and technological approaches. This hybridisation reflects a broader shift in the character of warfare, in which boundaries among domains, actors, and methods are increasingly blurred. At the global level, the implications are far-reaching. The proliferation of uncrewed systems and precision-strike technologies is likely to accelerate, creating new challenges for both military and civilian security. Non-state actors may gain access to capabilities previously reserved for state militaries, increasing the potential for disruption and instability in maritime regions worldwide.

Ultimately, the Black Sea campaign serves as a critical case study in the transformation of modern warfare. It demonstrates that adaptability, innovation, and effective technology integration can offset conventional disadvantages and reshape the balance of power. For military planners and policymakers, the key lesson is clear: success in future conflicts will depend not on preserving traditional models, but on anticipating and adapting to a rapidly evolving operational environment.

3.4 Cyber Domain of the Russia–Ukraine War

Russia's launching of its military annexation of Crimea in 2014 can also be considered the beginning of the world's first cyber war. At present, the term has no common definition. In this article, it is used to describe cyberattacks and operations which, for the first time, accompanied an open military invasion. Since the launch of Russia's full-scale invasion in February 2022, cyberspace has constituted an integral component of Russian operations, supporting military activities across multiple domains and contributing to a broader campaign aimed at disrupting Ukrainian governance, degrading critical infrastructure, shaping the information environment, and influencing strategic decision-making. Cyber operations have been employed as a force multiplier within Russia's wider approach to integrated campaigning, complementing conventional military actions through disruption, coercion, espionage, and information activities (Tkachuk 2025).

The cyber dimension of the conflict did not emerge in 2022 but was preceded by years of sustained hostile cyber activity directed against Ukraine. Ukrainian authorities reported approximately 288,000 cyber incidents during 2021, following more than 397,000 incidents recorded in 2020, with a significant proportion targeting government networks, public institutions, and critical services.

Following the initiation of large-scale combat operations, cyber activities intensified and became increasingly synchronised with military objectives. Between 2022 and 2024, Ukraine experienced numerous Distributed Denial-of-Service (DDoS) attacks, ransomware campaigns, destructive malware incidents, and cyber-enabled sabotage operations directed against critical national infrastructure, including the energy, transportation, telecommunications, and government sectors. The scale and frequency of these activities continued to increase, with cyber incidents rising by approximately 48 % between the first and second halves of 2024 (Olejnik 2025).

By 2025, the cyber battlespace had evolved into an increasingly complex operational environment characterised by both continuity and adaptation. While many attack vectors remained consistent with previous years, new threats, actors, and operational techniques emerged, challenging even Ukraine's highly developed cyber defence architecture. Throughout the first half of 2025, more than 80% of identified Russian cyber operations targeted civilian and dual-use infrastructure, particularly in the energy, logistics, telecommunications, and public administration sectors. Ukrainian authorities reported an average of approximately 16.5 cyber incidents per day, underscoring the persistent nature of the cyber campaign and its integration into Russia's broader strategy of strategic pressure (Tkachuk 2025).

The experience of the Russia–Ukraine War highlights the increasingly important role of cyberspace as an operational domain influencing military effectiveness, societal resilience, and strategic stability. Cyber operations are no longer merely supporting activities but have become an essential element of contemporary conflict, capable of generating operational and strategic effects without direct physical engagement. Consequently, the conflict has reinforced the requirement for NATO and European nations to develop comprehensive cyber defence and cyber deterrence postures that extend beyond traditional perimeter security measures. Effective resilience increasingly depends on the protection of critical infrastructure, secure supply chains, robust governance frameworks, and the integration of cyber resilience into national and Alliance-wide defence planning.

The broader Euro-Atlantic security environment has also been affected by the expansion of Russian cyber activities beyond Ukraine. During the past year, cyber operations attributed to Russian actors reportedly increased by approximately 25 % against NATO member states. Nine of the ten most frequently targeted countries were NATO Allies, with the United Kingdom accounting for approximately 12 % of observed activity and the United States approximately 20 %, compared with 11 % directed against Ukraine. The sectors most frequently targeted included government institutions, public services, information technology companies, research organisations, and academic institutions. Government entities accounted for approximately 25% of all Russian-attributed cyber activity, a significantly higher proportion than that associated with cyber operations attributed to other state actors, such as China, Iran, or North Korea (Microsoft 2025).

3.4.1 Summary of Cyber Incidents and Cyber Operations in 2024–2025

The period from 2024 to 2025 was characterised by a significant intensification of cyber activities associated with the Russia–Ukraine War. Cyber operations remained closely integrated with broader military and strategic objectives, targeting critical infrastructure, government institutions, and civilian networks. The cyber domain continued to serve as an operational environment for disruption, espionage, information operations, and strategic coercion. Several important trends can be identified during the 2024–2025 period:

1. Increasing Operational Tempo – The number of cyber incidents continued to grow, culminating in a 48% increase during 2024 and a sustained high rate of activity throughout 2025.
2. Shift Toward Civilian Infrastructure – Russian cyber operations increasingly targeted civilian and dual-use infrastructure rather than purely military systems, reflecting an effort to affect societal resilience and governmental functionality.
3. Integration with Strategic Objectives – Cyber operations remained synchronised with broader military, political, and informational objectives, supporting Russia's integrated campaigning approach.
4. Persistence of the Threat – The average of approximately 16.5 incidents per day during the first half of 2025 illustrates the continuous nature of cyber competition, with no clear distinction between wartime and peacetime activity.

The cyber activities observed during 2024–2025 demonstrate that cyberspace has become a permanent operational domain within contemporary armed conflict. The increasing number of incidents, the concentration on critical infrastructure, and the growing integration of cyber operations with strategic objectives confirm that cyber capabilities are now employed not merely as supporting tools but as instruments capable of generating operational and strategic effects. The experience of Ukraine underscores the importance of cyber resilience, critical infrastructure protection, and the integration of cyber defence into broader national and Alliance defence planning.

3.4.2 Artificial Intelligence and the Future of Cyber Conflict

Several emerging trends observed in 2025 have raised concerns about the resilience of both public and private digital infrastructure across Europe. Of particular significance is the increasing role of artificial intelligence (AI) as a force multiplier within cyberspace. The integration of AI into cyber operations is expanding across the entire cyber kill chain, from the generation of large-scale phishing and social engineering campaigns to the automation of vulnerability discovery, exploitation, lateral movement, and target reconnaissance.

AI-enabled tools are also increasingly capable of supporting the development of adaptive malware, dynamically modifying command-and-control architectures, and altering malicious code in real time to evade detection and defensive countermeasures.

The operational implications of these developments are substantial. By leveraging AI-enabled capabilities, threat actors can conduct highly scalable cyber operations across multiple sectors while significantly reducing the manpower, expertise, and time traditionally required for such activities. This trend is further accelerated by the widespread availability of open-source technologies and the increasing accessibility of advanced cyber tools. As a result, the barriers to entry for sophisticated cyber operations continue to decline.

Many experts assess that current AI models are already capable of supporting virtually every stage of cyber operations. Attention has therefore been directed toward the potential emergence of so-called Military AI Cyber Agents (MAICAs)—autonomous systems capable of operating independently throughout the entire cyber engagement cycle. Such agents could identify vulnerabilities, adapt tactics and techniques in response to defensive measures, conduct exploitation activities, and execute attacks against designated targets with limited human intervention. Critical infrastructure systems are considered particularly vulnerable to such threats due to their reliance on complex networks, legacy technologies, and operational systems that are often difficult to modernise or secure comprehensively.

The principal advantage offered by AI-enabled cyber capabilities lies in their ability to generate disproportionate effects with relatively limited resources. By exploiting vulnerabilities in interconnected critical infrastructure networks, hostile actors may cause significant operational disruption with only a limited number of cyber operators. This asymmetry creates a potentially powerful deterrence-by-denial challenge, particularly when attribution remains difficult and when cyber activities are conducted through proxies, affiliated groups, or state-sponsored actors operating below the threshold of armed conflict (Kott 2023).

A related conceptual shift is reflected in the White Paper on European Defence and the accompanying EU Defence Readiness 2030 initiative, which states that: “Both defensive and offensive cyber capabilities are needed to ensure the protection and freedom of manoeuvre in cyberspace” (EEAS 2025) This formulation reflects the growing recognition that cyberspace constitutes an operational domain in which states must possess not only defensive capabilities but also credible offensive capabilities to contribute to deterrence and operational freedom of action.

The development of such capabilities further underscores the increasing militarisation of cyberspace and introduces new dimensions to the traditional security dilemma. In an era characterised by an accelerating “race for innovation,” technological competition increasingly revolves around the development, acquisition, and deployment of advanced technologies that are simultaneously accessible, affordable, and inherently dual-use. Under such conditions, states often find it difficult to assess whether emerging technological capabilities are intended for defensive, commercial, or offensive military purposes. Technologies developed for legitimate civilian applications may be rapidly adapted for military or intelligence purposes, thereby increasing uncertainty and strategic mistrust among competitors.

This challenge is particularly evident in cyberspace, where the distinction between civilian and military applications is often blurred, and cyber capabilities have become an integral component of contemporary warfare. The experience of the Russia–Ukraine War demonstrates that cyber operations now routinely support military campaigns, influence decision-making processes, target critical infrastructure, and contribute to broader strategic objectives.

These developments also raise important conceptual and legal questions. If cyber capabilities are increasingly recognised as instruments through which force can be projected and strategic effects generated, then their employment must be considered within the framework of existing international law and international humanitarian law. Consequently, a key issue for policymakers, military planners, and legal experts is determining under what circumstances a cyber operation may constitute an “armed attack” under international law and how to interpret such thresholds, given the evolving experience of the Russia–Ukraine conflict. This question remains central to the future development of cyber deterrence, collective defence, and the application of legal norms in the cyber domain.

3.4.3 Institutionalisation of Cyber Defence

The growing scale, sophistication, and strategic impact of cyber operations observed throughout the Russia–Ukraine War have highlighted the need for a comprehensive response extending beyond purely technical or military measures. As cyber threats increasingly target critical infrastructure, governmental functions, and societal resilience, both NATO and the European Union have progressively adapted their policy, legal, and operational frameworks. The development of cyber defence capabilities, resilience mechanisms, and regulatory instruments reflects a broader effort to address cyberspace as a contested operational domain and an integral component of collective security.

The development of cybersecurity structures in Ukraine has been highly centralised. The organisations responsible for cybersecurity in Ukraine existed prior to 2014 (except for the national cyber police). They each had embedded cultures and relationships within the NSDC and Ukraine's power structures. Each of these organisations was already familiar with the limited-resource environment and was generally unable to circumvent it. The laws and processes established look good on paper. They align with European and NATO standards, but they are akin to bolting on new organisational structures and goals to existing frameworks. There are motivated individuals within each organisation. Each organisation expressed a strong and genuine interest in addressing cybersecurity concerns, yet, by necessity, had many other priorities that often superseded cybersecurity (Brantly 2018).

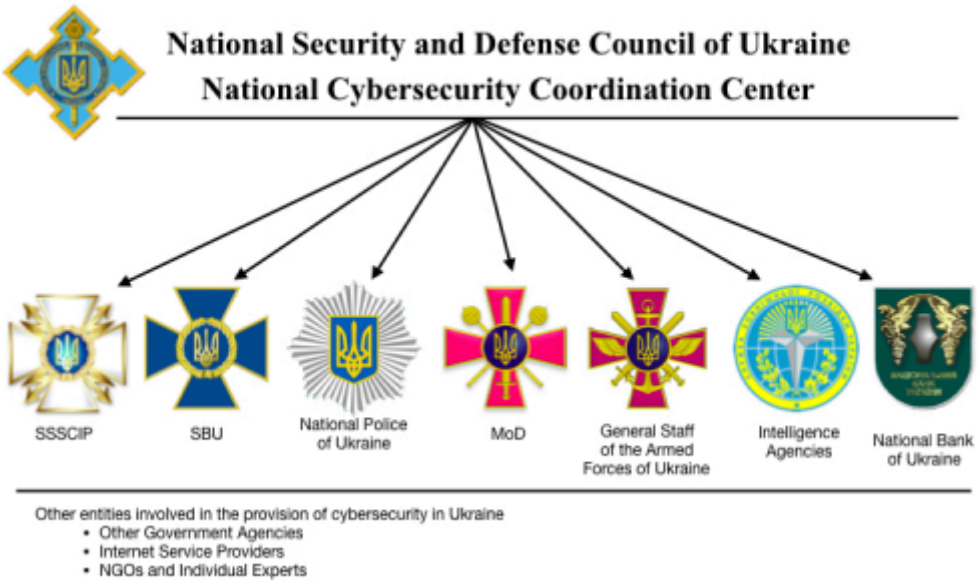

Figure 11: Organisation of National Cybersecurity in Ukraine (Brantly 2018)

In Europe, since the adoption of the Network and Information Systems (NIS) Directive, proposed in 2013 and entering into force in 2016, the European Union has progressively developed a comprehensive regulatory framework to enhance cyber resilience, strengthen cooperation among Member States, and improve the protection of critical infrastructure. The Directive established baseline cybersecurity requirements and mandatory incident-reporting obligations for operators of essential services and digital service providers, thereby laying the foundation for a more coordinated European approach to cybersecurity (European Commission 2016).

Significantly, these efforts coincided with NATO's formal recognition of cyberspace as an operational domain during the 2016 Warsaw Summit, placing cyberspace alongside the land, maritime, air, and space domains as an environment in which military operations may be conducted (Minarik 2016). This milestone reflected the growing recognition within the Alliance that cyber activities can generate operational and strategic effects comparable to those achieved in traditional domains. Following this development, numerous Allied nations revised their national cybersecurity and cyber defence strategies, while the European Union accelerated efforts to establish a more integrated and coherent framework for cyber governance.

A further step was the adoption of the Cybersecurity Act in 2019, which introduced a European cybersecurity certification framework designed to enhance the security, reliability, and interoperability of digital products, services, and information and communications technology systems throughout the EU Single Market. Building on this foundation, the European Commission presented the EU Cybersecurity Strategy for the Digital Decade in 2020, formalising a comprehensive approach that integrates technological, industrial, regulatory, and security dimensions of cyberspace. The strategy places particular emphasis on cyber resilience, recognising it as a critical enabler of strategic autonomy, economic security, and public trust in Europe's increasingly digitalised environment.

The strategic concepts outlined in the 2020 framework subsequently guided the evolution of European cyber policy and legislation, including the modernisation and expansion of the original NIS framework. This process reflects a broader shift toward an integrated model of cyber governance that aligns with NATO's emphasis on resilience, collective defence, and the protection of critical national infrastructure against increasingly sophisticated cyber threats. The experience of the Russia–Ukraine War has further reinforced the relevance of this approach, demonstrating that cyber resilience, secure digital infrastructure, and effective public-private cooperation are indispensable components of national and collective security in contemporary high-intensity strategic competition.

3.4.4 Future of European Cyber Deterrence

An assessment of the evolving cyber dimension of the Russia–Ukraine War demonstrates that cyberspace has become a fully-fledged operational domain, capable of generating strategic, operational, and tactical effects comparable to those achieved in the traditional domains of warfare. The conflict has highlighted that cyber operations are no longer confined by geographic boundaries.

Critical infrastructure, government networks, defence-related systems, and civilian digital ecosystems across Europe and NATO member states have increasingly become targets of hostile cyber activity, underscoring the transnational and interconnected character of contemporary cyber threats.

The widespread adoption of artificial intelligence, machine learning, and advanced automation, combined with the growing sophistication of both state-sponsored and non-state threat actors, has significantly increased the scale, speed, and complexity of cyber operations. These developments have amplified the asymmetry between attackers and defenders, enabling adversaries to conduct highly scalable and adaptive campaigns while exploiting vulnerabilities across military, governmental, and commercial networks. As a result, the traditional distinction between civilian and military assets is becoming increasingly blurred, particularly in the context of dual-use infrastructure. This reality reinforces the importance of accurately classifying cyber activities and determining when cyber operations may constitute an armed attack under international law, in a manner consistent with emerging legal and operational frameworks developed in response to contemporary conflicts.

The Ukrainian experience provides a particularly valuable case study in national cyber resilience and the integration of cyber defence. By establishing a comprehensive framework that combines governmental institutions, private-sector partners, volunteer cyber communities, and offensive cyber capabilities, Ukraine has demonstrated an effective approach to resilience, deterrence, and active cyber defence. The integration of public-private cooperation, rapid information sharing, and operational agility has enabled Kyiv to maintain the functionality of critical systems while countering persistent Russian cyber campaigns. This model offers important lessons for Allied nations seeking to strengthen their own cyber defence posture and highlights the value of a whole-of-society approach to cybersecurity.

At the European level, regulatory initiatives such as the NIS Directive and the Cyber Resilience Act[3] constitute significant steps toward a more integrated framework for cyber governance and digital security. Nevertheless, substantial challenges remain, including uneven levels of cyber maturity among Member States, dependencies on non-European technology providers, and the absence of fully integrated multinational cyber capabilities.

Addressing these shortcomings will require closer coordination, enhanced interoperability, and the continued development of collective cyber defence mechanisms.

In this context, proposals to strengthen existing multinational cyber structures and establish more robust European-level cyber command-and-control arrangements represent important components of a credible cyber deterrence posture. The lessons of the Russia–Ukraine War suggest that effective cyber deterrence cannot rely solely on defensive measures. Rather, it must integrate resilience, active defence, situational awareness, strategic communication, and, where appropriate, offensive cyber capabilities within a coherent framework of deterrence by denial and deterrence by punishment.

Ultimately, the development of an effective European cyber deterrence posture requires a comprehensive, multi-domain, and whole-of-government approach that integrates regulatory, technological, operational, and military instruments. Only through the coordinated employment of national and multinational capabilities can Europe effectively counter hybrid threats, strengthen collective resilience, and preserve strategic autonomy in an increasingly contested digital environment.

3.5 The Russia–Ukraine War and the Space Domain

The Russia–Ukraine War is not the first conflict in which space capabilities have supported military operations; however, it represents one of the first large-scale, high-intensity conflicts in which space-based capabilities have been integrated into military operations in a systematic and operationally significant manner. Space support has extended beyond traditional intelligence collection to include commercial space services, Satellite Communications (SATCOM), Positioning, Navigation and Timing (PNT), space-based ISR, EW activities targeting space-enabled systems, and competition within the space domain itself.

[3] The NIS Directive and the Cyber Resilience Act (CRA) are two core European Union legal frameworks designed to secure the digital supply chain. NIS2 focuses on the security of the organizations providing essential and important services, while the CRA focuses on the security of the products (hardware and software) placed on the market. The revised NIS-2 directive is aimed at companies and organisations that provide critical or important services. These include energy suppliers, banks, transport and healthcare companies, as well as manufacturers of goods (e.g. chemicals, mechanical engineering, etc.) and their suppliers.

The conflict, therefore, provides valuable insights into the evolving role of space as an operational domain in contemporary warfare (Ogden 2024). Prior to February 2022, major military powers had already recognised the strategic and operational advantages offered by space capabilities and had invested heavily in military and dual-use space systems (Pobjie 2026). Following the launch of Russia's full-scale invasion of Ukraine, the space domain rapidly became an integral component of the broader operational environment. Space assets played a critical role in enabling C2, ISR, precision targeting, strategic communications, and force employment.

At the same time, both Russia and Ukraine, supported by their respective partners and commercial actors, sought to protect their own space-enabled capabilities while degrading their adversary's capabilities through cyber operations, EW activities, and other counterspace measures. The conflict has highlighted the emergence of a contested, congested, and increasingly competitive space environment in which state and non-state actors, including commercial providers, contribute directly to military effectiveness. As such, the war offers important lessons on integrating space capabilities into joint operations and illustrates how the space domain has evolved from a supporting enabler to a critical component of military power and a potential domain of confrontation in future high-intensity conflicts.

3.5.1 Evolving Geopolitical Context of the Space Domain

The integration of space capabilities into military operations predates the Russia–Ukraine War. Many military analysts and defence scholars regard the Gulf War as the first conflict to demonstrate the decisive operational value of space-enabled capabilities, particularly by satellite-based ISR, communications, and navigation systems fully integrated into military planning and execution. Since then, reliance on space-based capabilities has become a standard feature of modern warfare, and the Russia–Ukraine War has further underscored their critical role in enabling military operations (Ogden 2024).

Over the past decade, the space domain has increasingly evolved from a supporting environment into a distinct operational domain. Armed forces worldwide have expanded investments in military space capabilities, recognising their importance for C2, ISR, PNT, missile warning, strategic communications, and precision targeting. However, the substantial financial and technological requirements associated with developing sovereign space capabilities have prevented many states from establishing comprehensive national space programmes. Consequently, numerous countries continue to rely on allied capabilities or increasingly on commercially provided space services (NATO 2019).

A significant transformation of the space sector has been driven by the rapid growth of commercial space actors. Large-scale private investment has accelerated the deployment of commercial satellite constellations and expanded access to space-based services. Systems such as Starlink, developed by SpaceX, exemplify the growing role of commercial providers in delivering resilient communications and other space-enabled capabilities.

The scale and responsiveness of commercial space enterprises have increasingly complemented—and in some cases exceeded—the capacity of national programmes to meet growing operational demands (OECD 2023).

These developments have enabled states lacking sovereign space capabilities to access critical space-enabled services when required. The experience of Ukraine following Russia's full-scale invasion in 2022 demonstrated how commercial space systems can rapidly provide operationally significant capabilities, including resilient satellite communications, geospatial intelligence, and enhanced situational awareness. The conflict has therefore highlighted the growing strategic importance of public–private partnerships and the expanding role of commercial actors in supporting military operations within the space domain (Bingen 2025).

3.5.2 Increasing Competition and Contestation in Orbit

As space-enabled capabilities become increasingly integrated into military operations, their protection has become a critical requirement. Space systems are inherently vulnerable to both natural hazards and deliberate hostile actions, making space security an increasingly important aspect of national defence planning. The growing dependence of military forces on space-based services has elevated concerns regarding the resilience and survivability of orbital assets in a contested operational environment.

Prior to the Russia–Ukraine War, concerns regarding counterspace capabilities had already intensified. A notable example was Russia's November 2021 direct-ascent anti-satellite test, during which a defunct satellite was destroyed by a Nudol missile system[4]. The event generated significant international concern due to the large amount of orbital debris created and its potential impact on the safety and sustainability of space operations. Such activities highlighted the increasing militarisation of the space domain and the potential consequences of kinetic counterspace operations. Beyond direct-ascent anti-satellite weapons, a broad range of counterspace capabilities can threaten space systems.

4 The Nudol missile system (PL-19) is a Russian ground-based, road-mobile anti-satellite and anti-ballistic missile system. It is the primary interceptor for the strategic defence system, designed to protect Moscow and to strike targets in Low Earth Orbit (LEO).

These include Rendezvous and Proximity Operations (RPO)[5] conducted by satellites operating in close proximity to foreign spacecraft; EW activities targeting satellite communications and navigation signals; cyber operations against space infrastructure; signal interception; spoofing; and various forms of electromagnetic interference.

Although many of these activities remain below the threshold of armed conflict, they possess the potential to disrupt or degrade critical military capabilities and strategic communications. Russia is widely assessed to possess a diverse portfolio of counterspace capabilities spanning kinetic, electronic, and cyber domains. Over recent years, Russian authorities have repeatedly tested and demonstrated these capabilities, reflecting a broader effort to enhance their ability to contest access to and use of the space domain. Such activities serve both operational and strategic purposes by signalling capability, deterring potential adversaries, and reinforcing Russia's status as a major space power, despite the technological and financial challenges facing its national space sector (Samson 2026).

The experience of the Russia–Ukraine War has reinforced the assessment that future high-intensity conflicts are likely to involve sustained competition within the space domain. Consequently, the protection of space assets, the development of resilient architectures, and the ability to operate effectively in a degraded space environment have become increasingly important components of military planning and force development.

3.5.3 Limited Space-Domain Effects at the Outset of the Conflict

The Russia–Ukraine War did not begin with a large-scale counterspace campaign involving the widespread destruction of satellites, extensive anti-satellite (ASAT) operations, or the systematic disruption of NATO space assets. Nevertheless, it would be inaccurate to conclude that the space domain was absent from the opening phase of the conflict. One of the first operations associated with Russia's full-scale invasion on 24 February 2022 was a cyberattack against the KA-SAT satellite[6] communications network operated by Viasat (Viasat 2022). The attack disrupted satellite communications terminals across Ukraine and parts of Europe, demonstrating the vulnerability of space-enabled infrastructure and highlighting the close integration of cyber and space operations in modern conflict. At the outset of the war, Ukraine possessed only limited sovereign space capabilities and relied heavily on foreign governmental and commercial providers for space-enabled services.

5 Rendezvous and Proximity Operations (RPO) are critical space manoeuvres where two or more spacecraft match orbits and navigate into close proximity to perform mission objectives. RPOs are essential for docking, satellite servicing (refuelling, repair), debris removal, and space station resupply.

6 KA-SAT is a high-throughput geostationary telecommunications satellite owned by Viasat. The satellite provides bidirectional broadband Internet access services

Russia, meanwhile, appeared to avoid actions that could have been interpreted as a direct attack on NATO space infrastructure, thereby limiting the risk of horizontal escalation beyond the immediate theatre of operations. This approach was broadly consistent with Moscow's initial political narrative, which portrayed the invasion as a limited "special military operation" rather than a broader interstate war.

As the conflict evolved, however, Russian official rhetoric increasingly characterised the war as a confrontation with the collective West, including the United States and NATO. This shift has reinforced concerns regarding the potential expansion of Russian counterspace activities and the increasing strategic importance of the space domain in the conflict.

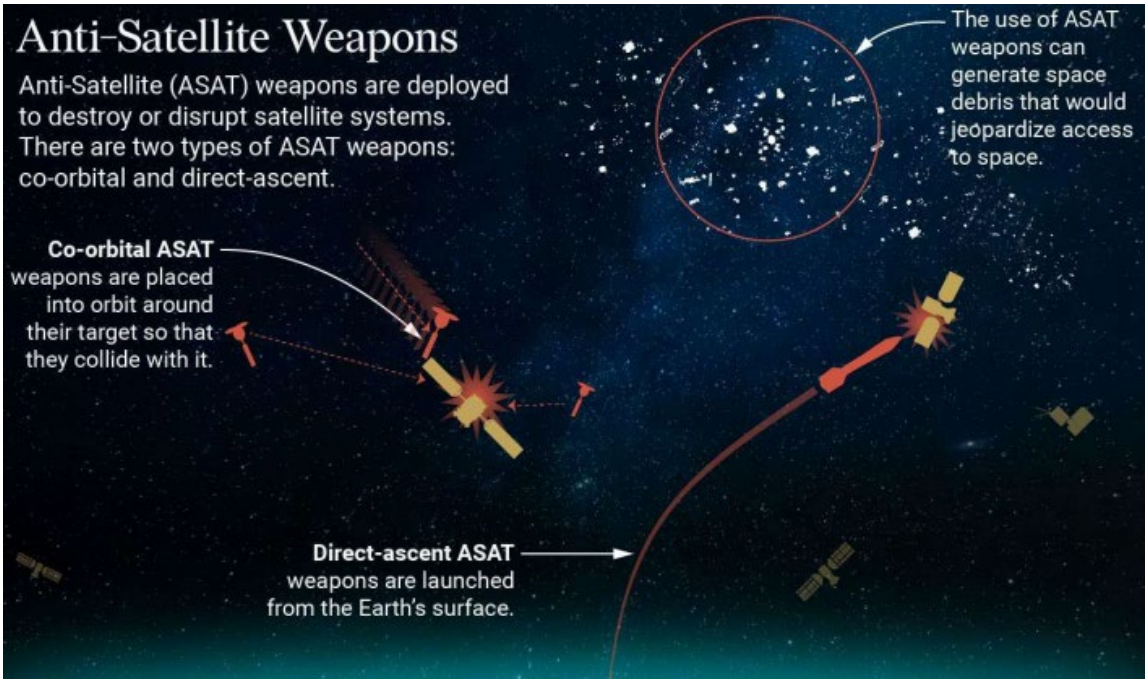

Figure 12: Anti-Satellite Weapons Effects (Weichert 2022)

3.5.4 Russian Space Component: Capabilities and Limitations

From the early stages of the war, both sides sought to secure access to space-enabled capabilities essential for military operations. This dynamic resulted in the emergence of two competing support networks. Russia relied primarily on its sovereign military and civilian space capabilities, while Ukraine benefited from extensive support provided by allied nations, commercial satellite operators, and international partners. Consequently, access to space-based ISR, SATCOM, PNT, and geospatial intelligence became an important factor shaping operational effectiveness.

The integration of military space capabilities into modern operations was pioneered by Western armed forces during conflicts such as the Gulf War and the Kosovo War. During the same period, Russia was recovering from the dissolution of the Soviet Union and focused primarily on maintaining its strategic nuclear deterrent while adapting to emerging forms of warfare. For many years, there was limited evidence regarding Russia's ability to integrate space-enabled capabilities into joint operations.

By the beginning of the Russia–Ukraine War, Russia possessed a relatively comprehensive portfolio of military and dual-use satellites supporting communications, ISR, missile warning, navigation, and electronic intelligence functions. However, several limitations remained evident. In particular, Russia's space-based Synthetic Aperture Radar (SAR) constellation was comparatively limited, reducing its ability to conduct persistent all-weather ISR operations. This capability gap was especially relevant in Eastern Europe, where cloud cover and adverse weather conditions frequently constrain optical satellite imagery.

Russia's invasion of Ukraine has forced Moscow to think differently and to apply unconventional strategies in the strategic domain of space. They've used the war as an excuse to enhance their military satellite capabilities and as a reason for deploying cutting-edge rockets that could revolutionise the launch business. These are complications for the West, but they are not necessarily direct threats. For that, one must analyse Moscow's development of its co-orbital satellites and other counterspace weapons (Weichert 2022).

Russia also sought to enhance the resilience of its PNT architecture by using alternative navigation and guidance methods alongside the GLONASS network[7]. Such measures reflected concerns regarding EW, signal interception, spoofing, and jamming in a highly contested electromagnetic environment (Baumann 2016).

[7] The GLONASS network (*Globalnaya Navigazionnaya Sputnikovaya Sistema*) is Russia's space-based global satellite navigation system. Operating similarly to the American GPS, European Galileo, and Chinese Bei Dou systems, it provides precise positioning, navigation, and timing data worldwide for both civilian and military users.

Figure 13: Russia´s Space Capabilities in the Ukraine War (Weichert 2022)

3.5.5 Operational Challenges and Adaptation

Although space-enabled capabilities contributed to Russian targeting and strike operations, their effectiveness was often constrained by broader operational shortcomings. Throughout much of the conflict, Russia faced challenges in C2, logistics, force coordination, battle damage assessment, and the availability of Precision-Guided Munitions (PGMs). As a result, the benefits provided by space-based ISR and navigation systems were not always translated into operational effectiveness (Dickey 2024).

By 2024–2025, however, Russian forces demonstrated gradual improvements in the integration of ISR, long-range precision fires, unmanned systems, and space-enabled targeting processes. Enhanced sensor-to-shooter linkages, improved reconnaissance-strike complexes, and more effective integration of multiple intelligence sources contributed to increased strike accuracy against critical infrastructure and operational-level targets. These developments suggest that Russia has continued to adapt its military space architecture and operational procedures, reinforcing the growing importance of space-enabled capabilities within a broader multi-domain approach to warfare.

From the earliest stages of the conflict, Ukrainian governmental institutions, defence organisations, and private entities sought access to foreign satellite-based capabilities. Commercial providers rapidly responded by supplying high-resolution geospatial intelligence, satellite imagery, and communications services. Companies such as Maxar Technologies and Planet Labs became important sources of commercial imagery intelligence, providing near-real-time situational awareness that supported strategic communications, intelligence analysis, and operational planning.

In parallel, commercial SATCOM services became a critical component of Ukraine's command-and-control architecture. The deployment of Starlink terminals enabled resilient, distributed connectivity across the battlespace, supporting C2, intelligence sharing, targeting processes, and coordination of military operations.

The availability of low Earth orbit (LEO) satellite communications significantly enhanced the resilience of Ukrainian communications networks, particularly in areas where terrestrial infrastructure had been degraded or destroyed.

As the conflict evolved, Ukrainian forces demonstrated considerable adaptability in integrating commercial technologies into military operations. Commercial SATCOM systems were employed not only for operational communications but also in support of unmanned systems, distributed command networks, and real-time intelligence dissemination. This development highlighted the increasing convergence of commercial innovation and military capability development, while simultaneously exposing the challenges associated with dependence on privately owned infrastructure (Dickey 2024).

The war has demonstrated that commercial space services can provide operationally significant capabilities traditionally associated with sovereign military systems. However, unlike national military assets, access to commercial capabilities remains dependent on business decisions, contractual arrangements, regulatory frameworks, and providers' willingness to support military operations. Consequently, the conflict has generated important debates within NATO and partner nations regarding the resilience, governance, and protection of commercially provided space-enabled services during armed conflict.

From a Russian perspective, the extensive integration of commercial space capabilities into Ukrainian military operations represented a significant operational challenge. The availability of commercial imagery, communications, and geospatial services substantially increased Ukraine's access to capabilities that would otherwise have required a mature sovereign space architecture.

3.5.6 Integrating Space Competition into Multi-Domain Operating Environment

During the initial phase of the Russia–Ukraine War, space-enabled capabilities and counterspace activities were rapidly integrated into a broader multi-domain conflict framework, particularly through cyber and EW effects targeting space systems and space-enabled services. In the cyber domain, one of the first major space-related incidents occurred on 24 February 2022, when Russian-linked cyber operations disrupted the KA-SAT satellite communications network operated by Viasat. The attack degraded satellite communications supporting Ukrainian government and military users and required large-scale remediation, including the replacement of tens of thousands of compromised user terminals. This incident demonstrated the operational vulnerability of commercial SATCOM architectures and their direct integration into the tactical and operational C2 environment.

Subsequent reporting in early March 2022 indicated that cyber intrusions were attempted against Russian space-related infrastructure and associated command networks, which Russian officials publicly framed as highly escalatory actions. In parallel, commercial space providers reported persistent cyber threats against satellite ground segments and user terminals, reflecting the growing interconnection between cyber operations and space-enabled military capabilities.

In the field of EW, Russian forces conducted sustained jamming and interference operations targeting Global Navigation Satellite System (GNSS) signals, including GPS and Galileo, affecting both Ukrainian and NATO activities in Eastern Europe. These actions were part of a broader electronic attack campaign designed to degrade the adversary's situational awareness, precision targeting, and force coordination within a contested electromagnetic environment (Bollfrass 2025).

Although a range of directed energy and counterspace systems have been publicly discussed in open sources, their operational deployment and effectiveness remain assessed with varying degrees of confidence within Western defence communities. Nevertheless, the broader pattern of Russian EW and space-related activity indicates an increasing emphasis on non-kinetic counterspace effects below the threshold of armed conflict escalation (Mowthorpe 2026).

These activities are frequently amplified within the information environment and contribute to strategic messaging and deterrence signalling. At the doctrinal level, Russian military writings have increasingly emphasised the importance of achieving information superiority and degrading adversary space-enabled capabilities as part of broader air and space campaign objectives. In this context, space is treated as an enabling layer within a wider integrated fires and effects framework rather than as a fully autonomous domain.

3.5.7 Future Military Implications for NATO

The Russia–Ukraine War demonstrates that future military operations will be increasingly dependent on access to resilient, responsive, and diversified space-enabled capabilities. The conflict has shown that space is no longer merely a supporting environment but an integral component of the operational battlespace, directly influencing C2, ISR, precision engagement, and strategic communications. At the same time, the war has highlighted the growing vulnerability of military operations to disruptions in satellite communications, PNT services, and space-based intelligence networks. Future conflicts are therefore likely to involve sustained competition for access to and freedom of action within the space domain, including the employment of cyber, EW, and other non-kinetic counterspace capabilities.

The increasing proliferation of commercial satellite constellations, particularly in LEO, is expected to enhance the resilience of space architectures by reducing reliance on a limited number of high-value assets. Consequently, military planners will need to prioritise distributed and redundant space systems, rapid reconstitution capabilities, and the ability to operate effectively in degraded or denied space environments. The conflict further suggests that integrating military, civil, and commercial space resources will become a defining feature of future high-intensity warfare, requiring new approaches to force development, operational planning, and space security.

For NATO, the Russia–Ukraine War has reinforced the strategic importance of space as an operational domain and highlighted the Alliance’s growing dependence on space-enabled capabilities across all operational domains. The conflict has demonstrated that maintaining operational effectiveness requires not only access to space-based services but also the ability to protect, defend, and rapidly restore those capabilities when challenged by adversary actions. As a result, resilience has emerged as a central requirement for future NATO space policy and capability development. Attention will need to be given to strengthening the protection of satellite communications, PNT systems, and space-based ISR networks against cyberattacks, EW activities, and other counterspace threats. The war has also underscored the critical role of commercial providers in supporting military operations, raising important questions regarding governance, contractual arrangements, legal frameworks, and the protection of privately owned infrastructure during armed conflict. Furthermore, the experience of Ukraine highlights the need for deeper integration of space operations into NATO’s conceptual and doctrinal framework, ensuring that space effects can be synchronised with activities in the land, maritime, air, cyber and space domains. Ultimately, the conflict confirms that the ability to secure access to space-enabled capabilities and to operate effectively in a contested space environment will become an increasingly important determinant of the Alliance's deterrence and defence.

3.6 Cross-Domain Dimensions of the Russia–Ukraine War

Within the context of the Russia–Ukraine War, the concept of cognitive warfare has re-emerged as an important analytical framework for understanding contemporary conflict. It describes the use of coordinated military and non-military instruments to influence perceptions, decision-making processes, and societal behaviour before, during, and beyond the conduct of kinetic operations. In this respect, cognitive warfare reflects the enduring principle articulated by Sun Tzu that strategic success can be achieved by shaping the conditions of conflict before military confrontation occurs (Hanzhang 1993).

3.6.1 Cognitive Dimension in the Russia–Ukraine War

The concept itself remains subject to significant academic and doctrinal debate. Historically, similar activities have been described by various constructs, including Psychological Operations (PSYOPS), subsequently redesignated in Western military terminology as Military Information Support Operations (MISO)[8], as well as Soviet and Russian concepts of active measures, which incorporated political influence, deception, disinformation, and covert action. These approaches were closely linked to the Russian tradition of *maskirovka*—the comprehensive employment of military deception—and later to the theory of reflexive control, which seeks to influence an adversary's decision-making process by shaping its perception of reality (Jones 2004).

Within Russian strategic thought, these activities are frequently incorporated into the broader concept of non-linear warfare, which integrates military, informational, political, economic, diplomatic, and other instruments of national power to pursue strategic objectives. Reflecting this approach, Russian Defence Minister Sergei Shoigu stated before the Academy of Military Sciences in 2019 that non-military measures may, under certain conditions, assume greater importance than the direct employment of military force (Nocetti 2024).

From a NATO perspective, cognitive warfare is generally understood as the synchronised employment of instruments of power to influence, protect, or disrupt human cognition, thereby affecting attitudes, behaviours, and decision-making processes and generating an operational or strategic advantage over an adversary. Russian practice, however, appears to adopt a broader and more holistic interpretation.

[8] According to US Joint Publication 3-13.2, published in 2014, Military Information Support Operations (MISO) are designed to develop and convey messages and devise actions to influence select foreign groups and promote themes to change those groups' attitudes and behaviours. MISO can also degrade the enemy's combat power, reduce civilian interference, minimize collateral damage, and increase the population's support for operations.

Russian information activities are directed not only at individual decision-makers and military audiences but also at entire societies and institutions, targeting political, economic, social, cultural, and informational dimensions simultaneously. Consequently, the Russia–Ukraine War extends far beyond the physical battlespace. Alongside military operations in the land, air, maritime, cyber, and space domains, the conflict is being contested within the information environment, where influence operations, strategic communications, disinformation campaigns, and cognitive effects have become integral components of broader campaigning efforts. In this regard, cognitive warfare serves as a force multiplier, supporting strategic objectives by shaping perceptions, influencing public opinion, undermining societal cohesion, and affecting decision-making at both national and international levels. At the international level, Russian information activities and interference campaigns can therefore be understood as elements of a broader strategy of strategic competition and coercion. By targeting human cognition and decision-making processes, these activities seek to generate effects that complement military operations while remaining below the threshold of direct armed confrontation. The growing significance of the cognitive dimension has prompted NATO and Allied nations to intensify efforts to develop concepts, doctrines, and capabilities designed to enhance resilience against influence activities and protect the integrity of decision-making processes.

While considerable attention has been devoted to developments on the battlefield, comparatively less emphasis has been placed on the strategic impact of Ukrainian resistance within the cognitive dimension. Ukraine's ability to withstand Russian aggression has challenged the perception of Russian military inevitability and strategic dominance that Moscow has sought to project internationally. Beyond its military significance, Ukrainian resistance has generated powerful strategic narratives that resonate both domestically and internationally. This resilience is perhaps best encapsulated by the Ukrainian word «*воля*» (volya), which simultaneously conveys the notions of will, freedom, and determination—qualities that have become central elements of Ukraine's strategic resilience and national resistance. Well before the large-scale invasion launched in February 2022, the operational environment in Ukraine had already been characterised by an ongoing conflict. This confrontation began in 2014, when the Russian Federation employed plausible deniability to conceal its involvement in a hybrid, multi-domain campaign to exert influence while avoiding formal attribution. Observers identified a progressive increase in non-kinetic and sub-threshold activities—including cyber operations, disinformation, and information manipulation—targeting Ukrainian civilian and military audiences, as well as Western societies and institutions, with the aim of creating ambiguity, shaping perceptions, and exacerbating societal polarisation (Dugoin-Clément 2025).

Russian actors have further enhanced their information warfare capabilities by integrating artificial intelligence. This has included the production of highly credible synthetic media (deepfakes), the dissemination of large volumes of tailored messaging across social media ecosystems, and the placement of fabricated content on Western digital platforms. In addition, generative AI systems have been deliberately exposed to and saturated with disinformation, increasing the risk of the inadvertent amplification of adversarial narratives.

The large-scale employment of these capabilities, whose cost-effectiveness has increased due to technological advances, supports multiple, mutually reinforcing operational objectives. Primarily, it enables a strategy of cognitive disruption aimed at degrading the integrity of individual and collective decision-making processes. Simultaneously, it seeks to influence the perceptions and decision calculus of political and institutional leaders, either deterring resistance to Kremlin objectives or encouraging alignment with them, depending on the operational context.

Consequently, any mechanism that safeguards the integrity of democratic processes, particularly the free and unhindered exercise of electoral choice, directly impedes Russian influence operations. Attempts at electoral interference have been repeatedly documented; however, such activities coexist with domestic constituencies that may be inherently receptive to political platforms aligned, wholly or in part, with strategic narratives compatible with the Kremlin's ideological orientation.

3.6.2 Russian Influence Operations and Strategic Narratives

Within the information dimension, Ukraine holds critical strategic significance. The country has chosen to align itself with the European socio-political model, which Moscow routinely portrays as "decadent" in contrast to the Russian model, presented as a defender of "traditional values" and a guarantor of order against the alleged disorder characteristic of Western societies.

For more than four years, Ukraine has borne a substantial cost for rejecting integration into the *Russkiy Mir* (Russian World), a multi-dimensional construct encompassing geopolitical, ideological, cultural, and societal dimensions. From Moscow's perspective, bringing Ukraine under its control would validate the perceived superiority of the Russian governance model. The ongoing Russification of occupied territories seeks to create the perception that local populations willingly identify with the Russian state and its socio-political framework. Such a narrative is intended to demonstrate the attractiveness of the Russian model and reinforce claims that Moscow offers a credible alternative to the broader Western order.

Establishing itself as such an alternative enhances Russia's ability to expand its international influence and challenge elements of the rules-based international order that it considers contrary to its strategic interests, particularly within multilateral institutions.

Conceptually, Ukraine represents an ontological challenge to Russian influence operations. This challenge may be encapsulated in the Ukrainian term *volya*, which carries the dual meaning of both "will" and "freedom." In Ukrainian political culture, the concept inherently associates individual and collective will with liberty, without requiring explicit qualification. This understanding stands in direct opposition to Russia's strategic objective of exercising control and influence over Ukraine. Russia's efforts to deny Ukraine's distinct political and national identity are therefore driven by several interrelated strategic considerations: imposing a preferred socio-political model that can be presented to partners in Africa and the Middle-East as an attractive alternative to Western and European governance; facilitating the revision of established norms of international law; and projecting great-power status through military force in order to offset perceptions of strategic failure resulting from the prolonged conflict in Ukraine.

By 2025, conventional warfare based on the application of military force will have become increasingly integrated with non-kinetic instruments, including cyber operations, economic coercion, and disinformation activities. Together, these instruments characterise the conflict as a manifestation of hybrid warfare. Within this context, the information environment has emerged as a key battlespace in interstate competition. Consequently, growing attention has been devoted to cognitive warfare—an approach that seeks to influence human cognition, shape perceptions, alter decision-making processes, and affect the interpretation of reality itself. It is within the information dimension that the Russia–Ukraine conflict intensified significantly in 2025. Long before the large-scale invasion in February 2022, both states were competing for dominance in the information environment and in the cognitive dimension of the battlespace, both domestically and internationally. Russia, a longstanding practitioner of information confrontation, has leveraged a centralised media ecosystem and extensive control over digital information flows to conduct large-scale influence and disinformation campaigns. These activities have sought to undermine Allied and Western cohesion by targeting public opinion, generating uncertainty, and eroding trust in institutions.

In responding to these operations, democratic states face an inherent vulnerability. Open societies and political systems founded upon the protection of freedom of expression provide adversaries with opportunities to penetrate the information environment and conduct influence activities. This creates a persistent challenge for NATO and its partners: safeguarding democratic values while simultaneously strengthening societal resilience against hostile information operations and cognitive threats.

3.6.3 The Russian Disinformation System

The concept of cognitive warfare encompasses a wide spectrum of activities, operations, and capabilities aimed at influencing, shaping, or disrupting an adversary's perceptions, decision-making processes, and behaviour by acting directly within the cognitive dimension of the operational environment. These activities seek to affect how individuals, groups, and institutions perceive reality, interpret information, and make decisions, thereby generating effects that can support broader political and military objectives. Within this framework, disinformation and misinformation are disseminated through both official and unofficial channels, exploiting social media platforms, artificial intelligence applications, and various information and communication technologies. Such efforts are typically conducted as part of long-term campaigns that may begin well before the outbreak of hostilities and continue throughout a conflict, supporting strategic, operational, and tactical objectives.

As illustrated in Figure 14, Russia's doctrine of information confrontation reflects this approach by integrating technical, informational, and psychological measures designed to influence target audiences, shape perceptions, undermine societal cohesion, and support the Kremlin's broader geopolitical and strategic objectives. Through the coordinated use of information activities, cyber capabilities, and psychological influence operations, Russia seeks to affect both decision-makers and public opinion, thereby shaping the operational environment in its favour (Voo 2025).

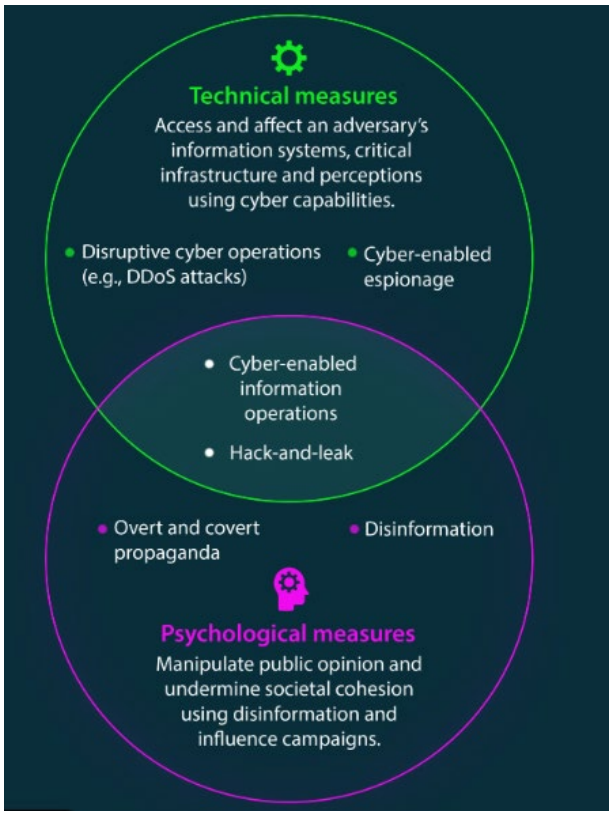

Figure 14: Russia's information confrontation ecosystem (Voo 2025)

In the Russia–Ukraine conflict, the Kremlin adopted from the outset an integrated approach that combines cognitive and information warfare capabilities with conventional military operations. Russia possesses a longstanding tradition of conducting influence activities and disinformation campaigns. Indeed, the term “disinformation” derives from the Russian word *dezinformacija* (дезинформация), which entered official usage during the early twentieth century. One of the most influential theoretical foundations underpinning Russian approaches to psychological influence is the concept of “reflexive control,” developed by the Russian mathematician and sociologist Vladimir Lefebvre in the late 1960s (Thomas 2010).

The cognitive control model is based on the premise that effective influence over a target population is achieved not through direct control of behaviour but through the manipulation of the underlying assumptions, beliefs, and cognitive frameworks that shape decision-making. The strategic objective is to induce individuals and groups to act in accordance with predetermined behavioural patterns while simultaneously degrading their critical thinking, situational awareness, and ability to identify ongoing manipulation efforts.

According to numerous analytical assessments and intelligence studies, the core principles of this theory continue to inform contemporary Russian influence operations and disinformation campaigns, albeit adapted to the realities of the digital information environment. The strategic intent remains consistent: to generate uncertainty, erode trust in democratic institutions and political leadership, undermine the credibility of Western governments and international organisations, and create divisions within both Allied societies and the broader target audience. By exploiting vulnerabilities in the information environment, these activities contribute to a broader campaign to shape perceptions, influence decision-making, and weaken political cohesion and societal resilience in support of Russian strategic objectives.

3.6.4 4D Model of Russian Information Operations

One of the principal mechanisms Russia employs to achieve its objectives in the cognitive dimension is the systematic dissemination of strategic narratives that often diverge from verifiable facts and are deliberately crafted to support its political and military aims. According to disinformation experts, Russian information operations can be analysed through the “4D” paradigm: Dismiss, Distort, Distract, and Dismay (MacAlpine 2025). This model provides a useful analytical lens for understanding the methods Russia employs to shape perceptions and influence domestic and international audiences.

The first element, Dismiss, seeks to undermine the credibility of opposing actors, institutions, or narratives. A common technique is whataboutism, whereby allegations or criticism are countered not by rebuttal but by redirecting attention to the accuser's alleged misconduct. This category also includes the use of informational pretexting, whereby Russian information channels disseminate claims that an adversary intends to conduct hostile actions in a specific area shortly before Russian forces themselves undertake such actions. Subsequently, previously disseminated information is cited as purported evidence supporting accusations against the adversary (Jordash 2025).

The second element, Distort, involves the deliberate manipulation of information to shape perceptions in a manner favourable to Russian objectives. This includes the dissemination of false, misleading, or selectively framed information. Linguistic framing plays a significant role in this process, as terminology is carefully selected to influence audience perceptions. For example, the term “special military operation” has been used instead of “war” or “invasion” to shape domestic and international interpretations of Russian military actions.

The third element, Distract, aims to saturate the information environment with competing narratives, misleading content, and information noise. Overwhelming audiences with large volumes of contradictory or low-quality information degrades the ability to identify reliable information. This approach frequently employs coordinated online activity, including automated accounts, bot networks, and other amplification mechanisms on social media platforms.

The fourth element, Dismay, seeks to generate fear, uncertainty, and psychological pressure to discourage resistance and reduce support for opposing positions. Such activities are intended to influence public attitudes and decision-making by creating a perception of inevitability, vulnerability, or futility in resisting Russian objectives.

Within the Russian Federation, the information environment is characterised by a high degree of state control, with information flows largely concentrated through official or state-aligned channels. Simultaneously, journalists and media organisations operate under increasingly restrictive legal frameworks governing so-called “fake news.” According to available reporting, nearly 50 Russian and Ukrainian journalists remain detained in Russian prisons, while many others have been compelled to relocate abroad. Even in exile, however, they remain subject to legal and administrative pressure through measures such as the “foreign agents” legislation, which targets selected non-governmental organisations, media outlets, and individuals receiving support from foreign institutions (Kolomychenko 2025).

Taken together, these activities illustrate how Russia integrates information operations, strategic communications, and psychological influence techniques into a broader campaign designed to shape the information environment, influence perceptions, and achieve strategic effects in support of national objectives. The main instruments and operational mechanisms of the Russian disinformation system are summarised in Table 4.

Table 4: Core Instruments of the Russian Disinformation System (Author)

Tool / Mechanism	Core Function	Key Methods	Technological Enablers	Target / Effects
Cognitive Warfare Framework	Influence perceptions and decision-making	Manipulation of beliefs, narratives, and cognitive frameworks	ICT infrastructure, social media, AI	Shapes reality perception, decision-making, and behaviour
Cognitive Control (Lefebvre)	Indirect behavioural control through mindset shaping	Altering assumptions, degrading critical thinking	Psychological models, propaganda techniques	Predictable behaviour, reduced awareness of manipulation
Integrated Information Confrontation Doctrine	Combine non-kinetic tools with military strategy	Coordination of cyber, informational, psychological measures	Cyber capabilities, media ecosystem	Strategic advantage, societal destabilisation
4D Model – Dismiss	Undermine credibility of adversaries	Whataboutism, pretexting, accusation redirection	Media channels, social platforms	Erosion of trust in opponents
4D Model – Distort	Manipulate reality and narratives	False information, selective framing, linguistic framing	State media, AI-generated content	Misperception of events, narrative control
4D Model – Distract	Overload information space	Bots, spam content, contradictory narratives	Botnets, automated accounts, algorithms	Confusion, reduced ability to identify truth
4D Model – Dismay	Induce fear and psychological pressure	Threat narratives, perception of inevitability	Media amplification, social networks	Demoralisation, reduced resistance
State-Controlled Information Environment	Control domestic narrative	Media regulation, censorship, legal pressure ("foreign agents")	State media, legal frameworks	Limited independent information, narrative monopoly
AI-Enabled Disinformation	Scale and automate content production	Deepfakes, fake articles, synthetic media	Generative AI, algorithm manipulation	Rapid spread of false narratives
Storm-1516 Operation	Undermine Ukraine & Western support	Deepfakes, burner accounts, fake websites	AI tools, social media networks	Delegitimisation of governments
Operation Doppelgänger	Impersonate trusted sources	Fake domains mimicking real media, AI-generated news	AI content generation, web cloning	Loss of trust in legitimate media
Operation Overload (Matryoshka)	Amplify disinformation via verification loops	Fake content sent to fact-checkers, identity appropriation	Multi-platform coordination, AI	Artificial credibility and amplification
Social Media Manipulation Infrastructure	Amplify narratives at scale	Coordinated posting, cross-platform replication	Telegram, X, TikTok, bots	Wide dissemination and normalisation of narratives
LLM / AI Training Data Manipulation	Influence AI-generated information	Seeding disinformation into datasets	Large language models, online content ecosystems	Biased AI outputs, long-term narrative embedding
Knowledge Ecosystem Pollution	Spread disinformation across platforms	Injection into encyclopaedias, web sources	Wikipedia, online databases	Persistent and recursive misinformation

3.6.5 Russia´s Key Cognitive Enablers

The domestic information-control measures have contributed to Russia's placement at 171st out of 180 countries in the 2025 World Press Freedom Index. In pursuit of its strategic objectives, Moscow increasingly integrates traditional information operations with emerging technologies, particularly artificial intelligence (AI) and AI-enabled automated systems (RSF 2025).

Generative AI is employed to manipulate, fabricate, and amplify a wide range of content, including images, translated texts, social media posts, and multimedia products. Beyond content generation, these capabilities can be used to influence the algorithms that shape information exposure on digital platforms and to support the creation of fraudulent websites designed to disseminate disinformation. AI-enabled influence activities have been extensively examined by fact-checking and counter-disinformation organisations such as NewsGuard[9], Viginum[10], and EUvsDisinfo[11]. These organisations have identified multiple information campaigns that employ artificial intelligence to facilitate the dissemination of false narratives, often serving as vectors for Kremlin-aligned propaganda.

Storm-1516 and Doppelgänger

One such campaign analysed by Viginum is Storm-1516, a Russian information manipulation operation designed to undermine the credibility of the Ukrainian government and reduce European support for Ukraine. In this case, elements of narrative denial and delegitimisation are particularly evident. Storm-1516 employed deepfake content, burner accounts—temporary, anonymous social media profiles used to disseminate information—and fraudulent websites that imitate legitimate news sources and promote pro-Kremlin narratives. The operation was also active during several electoral cycles, including the German elections in early 2025 (Viginum 2025).

[9] NewsGuard provides data, analysis and journalism that helps enterprises and consumers identify reliable information online.

[10] VIGINUM is the French State's technical and operational service dedicated to strengthening national protection against information manipulation.

[11] EUvsDisinfo is the flagship project of the European External Action Service's East StratCom Task Force. It was established in 2015 to better forecast, address, and respond to ongoing disinformation campaigns affecting the European Union, its Member States, and countries in the shared neighbourhood. EUvsDisinfo's core objective is to increase public awareness and understanding of the Kremlin's disinformation operations, and to help citizens in Europe and beyond develop resistance to digital information and media manipulation. Using data analysis and media monitoring services in 15 languages, EUvsDisinfo identifies, compiles, and exposes disinformation cases originating in pro-Kremlin media that are spread across the EU and Eastern Partnership countries.

The dissemination architecture supporting Storm-1516 is highly sophisticated and, at times, appears to intersect with other Russian influence operations. One closely related effort is Operation Doppelgänger (German for “double” or “evil twin”), a Russian disinformation campaign targeting Western audiences in the context of the Russia–Ukraine conflict. As part of Russia’s broader information warfare and hybrid influence activities, the operation seeks to shape perceptions and undermine support for Ukraine and its international partners.

Operation Doppelgänger relies on replicating legitimate media outlets and government websites by creating counterfeit domains that differ only slightly from authentic web addresses. Artificial intelligence is then employed to generate fabricated articles and supporting content that closely resemble legitimate reporting. The operation’s primary objective is to undermine trust in authoritative information sources, generate uncertainty within the information environment, and erode public confidence in democratic institutions across the Euro-Atlantic area.

Operation Overload (Matryoshka)

Another campaign that has attracted significant attention from fact-checking organisations is Operation Overload, also referred to as *Matryoshka* (Viginum 2024). This operation employs a multi-layered influence methodology. Initially, false or manipulated information—often generated or enhanced through AI tools—is disseminated online. Subsequently, journalists, researchers, and fact-checking organisations are prompted to verify the content, thereby amplifying its visibility within the information environment. Analysis conducted by the organisation CheckFirst[12] between 1 September 2024 and 31 May 2025 identified 704 emails sent to fact-checkers and researchers requesting verification of articles containing Russian propaganda narratives. The operation systematically appropriated the identities of Western public figures and legitimate websites to fabricate content, while replicating the same narratives across multiple channels to create the appearance of authenticity and independent corroboration (CheckFirst 2025). Operation Overload primarily exploits four digital platforms—Telegram, X (the social network), Bluesky, and TikTok—demonstrating the increasingly integrated use of social media ecosystems to support coordinated information operations.

[12] CheckFirst was founded in the first months of the global pandemic with the intention to help fight disinformation about COVID. Since then, CheckFirst was associated to many high-level projects in content monitoring or political ads monitoring as well as in the design of state-of-the-art research tools for data analysis and investigations.

Collectively, these campaigns illustrate the evolution of Russian information confrontation capabilities toward a technology-enabled model that integrates artificial intelligence, strategic communications, deception, and cognitive warfare techniques. Their overarching objective remains to achieve strategic effects in the information environment by influencing perceptions, undermining trust, degrading societal resilience, and shaping decision-making among target audiences.

Large Language Models and Information Manipulation

Over the past year, Russia has expanded its information operations toolkit to include the exploitation of Large Language Models (LLMs)—artificial intelligence systems trained on extensive text datasets to process, generate, and interpret human language. By systematically introducing disinformation and propaganda narratives into the digital information environment from which such systems draw information, Russian actors seek to influence the outputs generated by AI-enabled platforms. As a result, responses produced by these systems may, in certain circumstances, reflect narratives aligned with Russian strategic messaging rather than objectively verified information.

By 2025, AI-powered chatbots had become widely used sources of information, making the manipulation of the information ecosystem upon which they depend an increasingly important component of information warfare and cognitive operations. A NewsGuard assessment of this phenomenon found that the proportion of questions left unanswered by major chatbot systems declined from 31% in 2024 to 0% in 2025 (Sadeghi 2025). This improvement in responsiveness, however, has not been matched by a corresponding increase in information reliability. According to the same assessment, the rate at which AI systems generated inaccurate or false information increased from 18% to 35%, indicating that more than one-third of the generated claims lacked factual accuracy. NewsGuard[13] further reported that, in 33 % of the cases analysed through March 2025, chatbot outputs reproduced narratives originating from *Pravda*, the Russian state-aligned media network associated with the dissemination of pro-Kremlin disinformation (Sadeghi 2025).

Additional research conducted by CheckFirst identified instances in which online knowledge repositories, including digital encyclopaedias such as Wikipedia, reproduced information originating from the same disinformation ecosystem.

[13] NewsGuard combines human expertise and technology to provide data, analysis and journalism that helps enterprises and consumers identify reliable information online. NewsGuard helps consumers assess the reliability of sources they encounter online. NewsGuard's products are all produced using a combination of human analysis scaled by technology.

These findings suggest that false or manipulated content can propagate across multiple layers of the information environment, increasing the likelihood of amplification through both human and machine-mediated information channels.

Although inaccurate AI-generated content was initially viewed primarily as a consequence of the relative immaturity of emerging artificial intelligence technologies, subsequent research indicates that the issue is more deeply rooted in the structure and training methodologies of such systems. Russian information actors have increasingly exploited these systemic vulnerabilities, integrating them into broader influence operations designed to shape perceptions, reinforce strategic narratives, and influence decision-making within the cognitive dimension. Consequently, the manipulation of AI training data and information sources has emerged as an important element of contemporary information confrontation and cognitive warfare (Châtelet 2025).

3.6.6 NATO and EU Cognitive Resilience

As cognitive warfare increasingly emerges as a central component of strategic competition, democratic states and international organisations have been compelled to strengthen their resilience against hostile influence activities. The EU has consequently assumed a leading role in developing policy and regulatory responses to these challenges.

The EU's Response

In response to persistent Russian disinformation campaigns and broader influence operations, the international community has adopted a range of measures to strengthen resilience in the information environment and protect democratic institutions from hostile interference. As part of these efforts to counter cognitive warfare and information operations, the European Parliament adopted a resolution on 23 January 2025 condemning the use of Russian disinformation to justify the war against Ukraine (EU 2025).

The resolution rejected Russian attempts to legitimise military aggression through selective historical narratives and criticised Moscow for failing to acknowledge responsibility for crimes committed during the Soviet era. Furthermore, it accused Russia of attempting to revise historical interpretations in support of contemporary geopolitical objectives.

The resolution called for enhanced protection of democratic processes and the digital information environment against foreign interference, as well as the continued application of restrictive measures against media entities that disseminate state-sponsored disinformation (EU 2025).

Countering cognitive warfare in the era of artificial intelligence represents an increasingly complex security challenge. The Russia–Ukraine conflict has demonstrated the growing importance of the information environment as a contested operational dimension. Through the exploitation of digital technologies, social media platforms, artificial intelligence, and influence networks, state actors can conduct operations designed to shape perceptions, manipulate narratives, and influence decision-making processes far beyond traditional geographic boundaries.

While the cognitive dimension has long been a component of conflict, emerging technologies have significantly increased the scale, speed, and reach of information operations. The proliferation of synthetic media, AI-generated content, and coordinated disinformation campaigns has made it increasingly difficult—even for informed audiences—to distinguish verified information from manipulated or fabricated narratives. Through strategic communications, electoral interference activities, influence campaigns, and the cultivation of information footholds in politically and socially sensitive areas, Russia seeks to exploit societal vulnerabilities, undermine cohesion, and challenge the resilience of European institutions from within. The strategic objective extends beyond influencing perceptions of specific events. Rather, it seeks to erode trust in democratic governance, public institutions, and the broader rules-based international order. The case of Ukraine illustrates both the acceleration of these trends and the critical importance of societal and media resilience in countering sustained information warfare campaigns.

The European Union has responded with a range of regulatory and policy initiatives, including the Digital Services Act, which aims to enhance transparency and accountability in the digital ecosystem. Nevertheless, no regulatory framework can fully identify, prevent, or neutralise every cognitive attack while simultaneously preserving the fundamental freedoms that characterise democratic societies. As a result, strengthening resilience against cognitive threats requires a comprehensive, multi-layered approach that extends beyond legislation alone. Maintaining unity among European states remains a critical requirement. Fragmentation in national approaches to countering information threats would create exploitable vulnerabilities and provide strategic advantages to hostile actors. Consequently, coordinated action across the European Union and with international partners is essential to ensure a coherent response to cognitive and hybrid threats.

At the same time, the Union must continue to adapt its legal and regulatory frameworks to the rapidly evolving technological environment. This includes ongoing refinement of legislation governing artificial intelligence, digital platforms, and information integrity. Given the pace of technological innovation, regulatory measures require continuous review to remain effective against emerging threats.

A central challenge in this process is maintaining an appropriate balance between security and fundamental freedoms. Protecting freedom of expression, media independence, and civil and political rights—particularly during electoral periods, when information environments are especially vulnerable to manipulation—remains a core requirement of democratic resilience. Measures designed to counter foreign interference must therefore be transparent, proportionate, and applied consistently across the political spectrum.

Effective defence against cognitive warfare must also place citizens at its centre of gravity. Since many influence operations target human cognition directly, long-term resilience depends upon strengthening critical thinking, media literacy, and public awareness. Enhancing support for fact-checking organisations, independent journalism, strategic communications initiatives, and public education programmes can significantly improve society's ability to identify and resist disinformation and propaganda.

Ultimately, cognitive attacks represent a significant test of the resilience of European democracies. As the information environment becomes an increasingly contested battlespace, democratic societies must develop the institutional, technological, and societal capacities necessary to detect, withstand, and recover from hostile influence activities. In this regard, societal resilience functions as a form of strategic defence—an essential safeguard for preserving democratic values, institutional legitimacy, and social cohesion in the face of persistent hybrid and cognitive threats.

NATO and Cognitive Warfare

For NATO, cognitive warfare represents the convergence and evolution of information-related activities, integrating traditional information warfare capabilities with concepts from psychology, cognitive science, neuroscience, systems theory, and complexity theory to support military and strategic objectives. It operates at the intersection of two functional areas that have historically been addressed separately: on the one hand, psychological operations (PSYOPS) and broader influence activities designed to affect perceptions, attitudes, and behaviour; and on the other, cyberspace operations, which seek to disrupt, degrade, manipulate, or destroy information systems and digital infrastructure (Allen 2018).

Operational experience demonstrates that success in the physical dimension alone is often insufficient to achieve strategic and political end states. While military operations can reduce an adversary's combat power and freedom of action, they do not necessarily secure lasting effects within the human dimension of conflict. Contemporary security challenges increasingly involve ideological competition, identity-based narratives, religious beliefs, political legitimacy, and societal cohesion—factors that cannot be addressed solely through military force. In some cases, the use of advanced military capabilities may even lead to unintended consequences, including increased resistance, radicalisation, or the emergence of new adversaries.

Consequently, challenges within the cognitive dimension cannot be resolved through operations in the physical dimension alone. As conceptualised by several of NATO's strategic competitors, dominance within the perceptual and cognitive dimension requires the integration of multiple elements, including self-awareness of national strengths and vulnerabilities, understanding of adversary behaviour and motivations, knowledge of the human environment, intelligence collection and analysis, psychological influence, information superiority, and the ability to shape or constrain an adversary's decision-making processes and strategic will.

Within the framework of MDO, the cognitive dimension increasingly emerges as the decisive arena in which strategic outcomes are ultimately determined. It is through human cognition that information is interpreted, decisions are made, and political and military actions are authorised. Despite its importance, however, the human dimension has frequently received less attention in the traditional physical domains. Recent conflicts have highlighted both the difficulty of achieving strategic objectives through military means alone and the consequences of insufficient understanding of complex human environments.

Campaigns such as those conducted in Afghanistan demonstrated that tactical and operational success does not automatically translate into strategic success if the social, cultural, political, and cognitive dimensions of the operational environment are not adequately understood and addressed. These experiences underscore the growing importance of cognitive warfare as a means of shaping perceptions, influencing behaviour, strengthening resilience, and achieving strategic effects across the full spectrum of competition and conflict (Allen 2018).

While the objective of cognitive warfare extends beyond the degradation of adversary military capabilities to include the targeting of societies, populations, and decision-making systems, it can be characterised as a persistent, below-threshold "shadow competition" conducted across multiple domains of engagement. Countering such activities requires a comprehensive whole-of-government approach that integrates all instruments of national power.

As previously noted, contemporary conflict is increasingly defined less by the use of kinetic force and more by the ability to generate, control, and contest influence within the information and cognitive dimensions. To shape perceptions and maintain narrative superiority in this type of confrontation, states must be prepared to operate in the cognitive dimension through coordinated national-level action that involves all relevant government stakeholders.

This necessitates enhanced synchronisation between the application of military force and other instruments of national power—diplomatic, informational, economic, and security-related—across the government. In practical terms, this may require adjustments to how defence capabilities are resourced, structured, and employed, with an emphasis on developing capabilities that operate below the threshold of armed conflict while simultaneously strengthening the armed forces' contribution to national and societal resilience.

For NATO, effective engagement in the cognitive dimension also depends on sustained interoperability and coordination among Allies. This is essential to ensure strategic coherence, reinforce credibility, and enable a synchronised response to hybrid and cognitive threats across the Alliance.

From a military perspective, addressing the full spectrum of challenges posed by cognitive warfare requires an integrated, multidimensional approach. This includes, first and foremost, investment in the scientific foundations of cognitive influence. A deeper understanding of human cognition is a key enabling factor in cognitive warfare, requiring sustained investment in cognitive science and neuroscience to support both defensive (protective) and, where appropriate, proactive capabilities.

Defining the human dimension as a distinct factor within the operational environment further necessitates integrating expertise from disciplines such as anthropology, ethnography, history, psychology, and the broader social sciences and humanities. These fields are increasingly required to work in close cooperation with military structures, for example, by translating large-scale quantitative data into actionable qualitative insights relevant to the operational environment.

In this context, recognising the cognitive and human dimensions as operational factors implies a broader reassessment of the relationship between technical and scientific disciplines and the social sciences and the humanities. Rather than operating in isolation, these factors must be integrated to enable a comprehensive understanding of adversary behaviour, societal dynamics, and influence mechanisms, thereby supporting decision-making and operational effectiveness.

3.6.7 Future Challenges in the Cognitive Dimension

The rapid development of cognitive technologies has significantly enhanced the capacity to analyse, process, and exploit information with unprecedented speed and precision. Achieving timely, informed, and resilient decision-making in contemporary security environments increasingly requires more than the application of human cognitive abilities alone. It necessitates integrating systems engineering with social sciences disciplines—including sociology, anthropology, criminology, and political science—to understand and respond effectively to the complexities of the modern, multi-domain operational environment (Diaz 2021).

In this context, the development of Computational Social Science offers important opportunities for modelling human behaviour and social dynamics. By integrating data-driven analytical methods with insights from the social sciences, this approach can improve understanding of the behaviour of both adversarial and friendly actors, as well as the broader human environment in which military and political competition take place. Such capabilities can support decision-makers by providing a more comprehensive assessment of societal trends, mechanisms of influence, and behavioural patterns relevant to strategic competition and conflict (Diaz 2021).

For NATO and Allied nations, these developments underscore the need to anticipate and address the full spectrum of challenges associated with cognitive warfare. Failure to understand and counter adversary activities within the cognitive dimension could significantly undermine the resilience, cohesion, and decision-making capacity of democratic societies.

As strategic competition increasingly shifts toward influence, perception management, and information advantage, the ability to operate effectively within the cognitive dimension becomes a critical component of deterrence and defence. Figure 15 illustrates the main aspects of Cognitive Warfare, indicating that it may target human cognition (military and civilian populations) as well as artificial cognition.

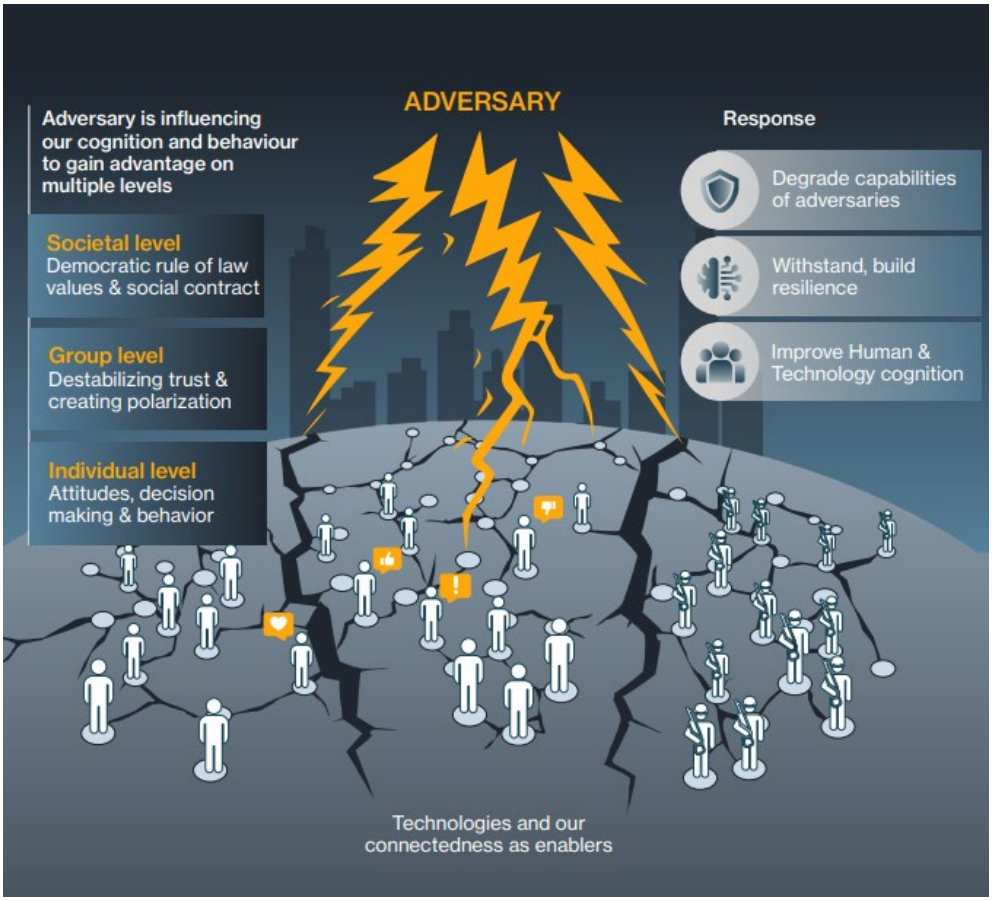

Figure 15: The Main Aspects of Cognitive Warfare (OCS 2025)

If NATO does not establish a sustainable, proactive framework for understanding and operating in the cognitive dimension, the Alliance may be compelled to rely more heavily on kinetic responses to address challenges that could otherwise be mitigated through non-kinetic means. While conventional military capabilities remain essential for achieving tactical and operational objectives, enduring strategic success increasingly depends on the ability to influence perceptions, shape decision-making, strengthen societal resilience, and contest adversarial influence in the cognitive environment.

Historically, technological innovation has consistently driven changes in military organisations, operational concepts, and doctrine. Today, rapid advances in neuroscience, cognitive science, artificial intelligence, biotechnology, and the broader convergence of NBIC technologies (Nanotechnology, Biotechnology, Information Technology, and Cognitive Science) are creating new opportunities and vulnerabilities in the cognitive dimension. These developments require NATO to maintain a heightened awareness of emerging threats and opportunities associated with cognitive warfare.

Not all Allied nations have yet fully recognised the implications of this evolving character of conflict. Consequently, the formal recognition of the cognitive dimension as an operationally relevant area serves not only as a conceptual development but also as a means of increasing awareness across the Alliance regarding the changing nature of warfare and strategic competition.

To address these challenges effectively, NATO should further integrate human situational awareness into existing situational awareness and decision-support processes. Understanding the attitudes, perceptions, motivations, and behavioural dynamics of populations, adversaries, partners, and other actors should become a complementary element of the Alliance's broader understanding of the operational environment.

Given that NATO remains in the early stages of conceptualising and operationalising the cognitive dimension, a key priority should be developing a common, comprehensive understanding of its scope, characteristics, and implications. This requires a shared conceptual framework across the Alliance, supported by continuous assessment of emerging threats, vulnerabilities, and opportunities arising from scientific and technological developments. Maintaining such an understanding will be essential for ensuring that NATO remains capable of adapting to the evolving security environment and effectively countering challenges within the cognitive dimension (Diaz 2021).

3.7 Synthesis of Key Factors of the Multi-Domain Operating Environment

The preceding analysis demonstrates that the operating environment of the Russia–Ukraine War has evolved into a highly complex multi-domain operating environment in which operational success is no longer determined by superiority in a single domain but by the ability to integrate and synchronise military capabilities across all operational domains. Although the land domain remains decisive for achieving territorial control and military-strategic objectives, developments between autumn 2023 and the end of 2025 confirm that operations conducted in the land, air, maritime, space, and cyberspace domains have become indispensable enablers of operational effectiveness. Simultaneously, force generation, defence-industrial capacity, technological innovation, economic resilience, and sustained international support have become critical components of national combat power, directly influencing operational endurance and strategic freedom of action.

The conflict further demonstrates that the distinction between the tactical, operational, and strategic levels of warfare has become increasingly compressed. Long-range precision strike capabilities, integrated ISR, autonomous and unmanned systems, cyber operations, and information activities routinely generate effects across multiple domains while simultaneously influencing military operations, national resilience, and strategic decision-making. Consequently, the contemporary operating environment is characterised by the continuous convergence of kinetic and non-kinetic activities requiring the synchronisation of military and non-military instruments to generate complementary operational effects.

Another defining characteristic of the conflict is the transition towards protracted attrition warfare, in which the ability to sustain combat operations has become as important as the ability to conduct them. Operational effectiveness is increasingly determined by the capacity to generate, regenerate, employ, and sustain combat power under conditions of prolonged high-intensity conflict. Force generation, personnel replacement, logistics, defence-industrial mobilisation, ammunition production, equipment regeneration, and societal resilience have therefore become decisive operational variables. The campaign demonstrates that success in contemporary warfare depends not solely on battlefield performance but equally on maintaining operational endurance, preserving combat effectiveness, and sustaining freedom of action over time.

The conflict has also confirmed that technological adaptation has become a principal driver of operational evolution. The rapid integration of UAS, autonomous strike capabilities, electronic warfare, artificial intelligence-enabled decision support, commercial space services, precision-guided munitions, and distributed command-and-control architectures has significantly increased the tempo of adaptation by both belligerents. Continuous modification of tactics, techniques, and procedures (TTPs) has become essential for preserving survivability, maintaining combat effectiveness, and exploiting temporary operational advantages. The resulting cycle of adaptation and counteradaptation has become a defining feature of the contemporary operating environment.

The key factors shaping the Multi-Domain Operating Environment are synthesised in Table 5. The table summarises the decisive factors that significantly impact each operational domain and assesses their contribution to achieving the expected operational effect.

Table 5: Key Factors Shaping the Multi-Domain Operating Environment in Ukraine (2024–2025) (Author)

Operational Domain	Key Factors	Expected Operational Effects
Land	• Operational Adaptation; • Attrition warfare; • Layered defence; • Extensive fortifications; minefields; • Unmanned vehicles and drones; • Dispersed defensive positions; • Force generation and regeneration; • Artillery superiority; • Force Generation and Mobilisation; • Logistics and Sustainment; • Deep Strike Capability; • Integrated ISR	• Continuous adaptation of tactics, techniques, procedures (TTPs), and force structures has become essential for maintaining combat effectiveness in a rapidly evolving operating environment. • Remain the decisive domain for territorial control. • Dense defensive systems and persistent indirect fires have significantly constrained combined manoeuvre, favouring attritional operations and incremental territorial gains. • Operational success increasingly depends on sustainment, personnel replacement, and preservation of combat power rather than rapid manoeuvre. • Determine the ability to replace losses, regenerate combat power, and sustain prolonged attritional warfare. • Critical enabler of operational endurance, freedom of action, and the maintenance of operational tempo. • Enable disruption of adversary C2, logistics, defence-industrial capacity, and critical infrastructure across domains. • Serves as the principal enabler for precision engagement, decision superiority, and cross-domain integration.
Air	• Contested airspace; • Integrated air defence (IADS); • Long-range precision strikes; • Glide bombs (FAB-1500); • Attack helicopters; • Limited availability of combat aviation • Logistics and Sustainment; • Deep Strike Capability; • Integrated ISR	• Absence of air superiority prevents large-scale offensive manoeuvre by either side. • Air power primarily supports deep strike, interdiction, suppression of air defences, and battlefield isolation rather than achieving air dominance. • Russian stand-off strike capabilities provide a significant operational advantage. • Critical enabler of operational endurance, freedom of action, and the maintenance of operational tempo. • Enable disruption of adversary C2, logistics, defence-industrial capacity, and critical infrastructure across domains. • Serves as the principal enabler for precision engagement, decision superiority, and cross-domain integration.
Maritime	• Long-range maritime strike systems; • Anti-ship missiles; • Naval drones (USV); • Protection of maritime logistics; Black Sea control; • Integrated ISR	• Maritime operations have shifted from fleet-centric operations to long-range precision engagement and autonomous systems. • Ukraine has denied Russia uncontested maritime freedom of action despite limited conventional naval capabilities, preserving strategic sea lines of communication. • Serves as the principal enabler for precision engagement, decision superiority, and cross-domain integration.
Space	• Satellite ISR; • Satellite communications (Starlink); • Satellite navigation (GNSS); • Commercial space capabilities; • Integrated ISR	• Space capabilities provide persistent ISR, precision targeting, secure communications, navigation, and battle damage assessment. • Commercial space assets have become operationally indispensable and significantly accelerate decision-making cycles and targeting processes. • Serves as the principal enabler for precision engagement, decision superiority, and cross-domain integration.
Cyberspace	• Cyber-attacks and offensive cyber operations; • Cyber defence; protection of critical infrastructure; • Electronic warfare (EW); jamming; • GNSS spoofing; electromagnetic spectrum management; counter-UAS; • Integrated ISR	• Cyber operations support strategic disruption, intelligence collection, information superiority, and protection of military networks. • Although rarely decisive independently, cyber effects significantly enhance operations in all other domains. • Control of the electromagnetic spectrum has become essential for ISR, drone employment, precision strike, and command and control (C2). • Continuous adaptation in EW creates a dynamic technological competition between both belligerents. • Serves as the principal enabler for precision engagement, decision superiority, and cross-domain integration.

Table 6 identifies the key factors in operational dimensions that shape the multi-domain operating environment. These factors influence all operational domains and have a decisive impact on operational effectiveness, operational endurance, force sustainment, combat power generation, and the ability to seize, retain, and exploit the initiative throughout a prolonged high-intensity campaign.

Table 6: Key Factors of Operational Dimensions Influencing Operational Domains in Ukraine (Author)

Operational Dimension	Key Factors	Operational Significance
Information	• Strategic communications; • Psychological and information operations; • Deception, social media and influence campaigns	Information has become a strategic capability shaping domestic resilience, international political support, mobilisation, and adversary decision-making. Information operations directly influence operational legitimacy and coalition cohesion.
Cognitive Human	• Morale; leadership; societal resilience; • Political will; • Personnel sustainability; mobilisation	Human factors increasingly determine long-term operational endurance. Combat motivation, force cohesion, public support, and political resilience directly influence force generation, operational effectiveness, and strategic endurance.
Physical Technological	• Artificial intelligence; • Autonomous systems; • Rapid innovation cycles	Technological adaptation continuously changes tactical and operational methods. Low-cost autonomous systems increasingly provide disproportionate operational effects while shortening innovation cycles and reducing the traditional advantage of expensive military platforms.

3.7.1 Analytical Conclusion

The partial analytical conclusion confirms that, while the land domain remains decisive for achieving military-strategic objectives through terrain control, operational success increasingly depends on the effective integration and synchronisation of capabilities across all domains. The Russia–Ukraine War demonstrates that contemporary high-intensity warfare is fundamentally characterised by the convergence of effects generated in the land, air, maritime, space and cyber domains. Within this environment, force generation, sustainment, integrated ISR, long-range precision strike, defence-industrial resilience, technological adaptation, and societal resilience have emerged as the principal determinants of combat power, operational endurance, and the ability to maintain the initiative. These developments provide compelling evidence that the character of warfare is evolving towards the principles underpinning respective NATO concepts and doctrines. Although the conflict continues to display many characteristics of industrial-age attrition warfare, it simultaneously illustrates that future military effectiveness will increasingly depend upon the ability to integrate capabilities across domains, generate decision advantage, preserve freedom of action, disrupt adversary decision-making, and continuously adapt force structures, capabilities, and operational concepts to an increasingly contested and dynamic operational environment. Consequently, the Russia–Ukraine War represents one of the most comprehensive contemporary case studies for the further development of NATO operational art, capability development, force design, and operational planning for future multi-domain, high-intensity conflict.

4. STRATEGIC ADAPTATION TO ATTRITION WARFARE

The evolving operating environment has compelled both Russia and Ukraine to continually adapt at the tactical, operational, and strategic levels. Such adaptation extends far beyond battlefield tactics. It encompasses the development of operational concepts and doctrines across the various warfighting functions, influencing force employment concepts, defensive architectures, long-range strike operations, command-and-control arrangements, industrial mobilisation, and the integration of emerging technologies. The conflict demonstrates that attrition warfare is not merely a consequence of operational stalemate but also a deliberate strategy through which belligerents seek to exhaust an opponent's military, economic, and political capacity to continue operational activities and engagement of respective military power.

The following sections examine the principal characteristics of this adaptation. They analyse how Russian forces have adjusted their operational methods to sustain offensive pressure amid heavy attrition; how Ukraine has developed a resilient, distributed defensive system designed to preserve combat effectiveness; and how both sides employ long-range strike capabilities to generate effects across the operational and strategic depth of the battlespace. Together, these developments provide important insights into the future character of warfare and the challenges that attrition-based conflicts may pose for NATO military planning.

The Russia–Ukraine War demonstrates that adaptation has become a decisive prerequisite for sustaining combat effectiveness in a highly contested and attritional operating environment. The principal areas of strategic adaptation undertaken by both belligerents are summarised in Table 7.

Table 7: Principal Factors of Strategic Adaptation in Attrition Warfare (Source: Author)

Area of Adaptation	Russian Adaptation	Ukrainian Adaptation	Strategic Significance
Operational Approach	Transition from large-scale manoeuvre operations to attrition-based warfare, emphasising sustained pressure and gradual advances.	Development of a defence-in-depth approach focused on preserving combat power and imposing attrition on attacking forces.	Demonstrates the centrality of endurance and resource management in high-intensity warfare.
Force Employment	Use of decentralised assault groups supported by artillery, drones, and electronic warfare rather than large, mechanised formations.	Distributed deployment of forces across mutually supporting defensive positions and fortified sectors.	Reduces vulnerability to precision strikes and enhances battlefield survivability.
Defensive Architecture	Increasing use of prepared defensive belts and fortified positions in occupied territories.	Multi-layered trench systems, obstacle belts, minefields, reserve positions, and concealed fortifications.	Reinforces battlefield resilience and complicates offensive operations.
Unmanned Systems (UAS)	Extensive employment of reconnaissance drones, loitering munitions, and one-way attack UAS to support offensive operations.	Large-scale integration of UAS for ISR, target acquisition, fire correction, and precision strikes.	Establishes drones as a central component of contemporary combat operations.
ISR–Strike Integration	Integration of ISR assets with artillery and long-range fires to accelerate targeting cycles.	Exploitation of Western intelligence support, combined with organic ISR networks.	Increases battlefield transparency and shortens sensor-to-shooter timelines.
Long-Range Strike Operations	Sustained missile and UAS campaigns against Ukrainian critical infrastructure, energy networks, and logistics systems.	Deep-strike operations against military bases, airfields, defence-industrial facilities, refineries, ports, and logistics nodes within Russia.	Extends competition into the operational and strategic depth of the battlespace.
Air and Missile Defence Competition	Use of massed strike packages designed to saturate and deplete Ukrainian air-defence systems.	Layered air-defence architecture integrating Western systems and adaptive interception concepts.	Highlights the growing contest between offensive strike capabilities and defensive protection systems.
Electronic Warfare (EW)	Extensive use of EW to disrupt communications, navigation, ISR systems, and precision-guided weapons.	Adaptation of communications networks and increasing integration of EW into defensive operations.	Confirms EW as a critical enabler of modern joint operations.
Command and Control (C2)	Greater decentralisation of tactical decision-making and adaptation to contested electromagnetic environments.	Flexible and distributed command arrangements supported by digital communications and mission command principles.	Improves operational responsiveness and resilience under persistent attack.
Industrial Mobilization	Expansion of defence production and force-generation mechanisms to sustain attritional warfare.	Growth of domestic defence production, drone manufacturing, and reliance on Western military assistance.	Demonstrates that industrial capacity is a decisive element of long-term military effectiveness.
Air-Surface Integration	Increasing integration of fires, drones, EW, and ground manoeuvre at lower tactical levels.	Integration of ISR, fires, air defence, EW, and UAS within tactical formations.	Reshapes combined-arms warfare and accelerates decision cycles.
Force Protection and Survivability	Greater dispersion, concealment, and adaptation to persistent surveillance.	Extensive use of camouflage, deception, fortified positions, and dispersed logistics.	Reflects the impact of a highly transparent battlespace.
Cognitive and Psychological Effects	Long-range strikes and information activities aimed at reducing Ukrainian resilience and morale.	Deep strikes against targets in Russia, designed to challenge perceptions of Russian invulnerability.	Demonstrates the growing importance of the cognitive dimension of warfare.
Strategic Sustainability	Reliance on manpower reserves, industrial capacity, and prolonged attrition to exhaust the adversary.	Focus on preserving combat power, sustaining international support, and maximising cost-effectiveness.	Illustrates that strategic endurance has become as important as battlefield success.

4.1 Russian Operational Adaptation

Traditionally oriented toward offensive operations, the Russian Armed Forces have conducted a highly attritional form of warfare in Ukraine, characterised by extensive use of massed fires and sustained personnel-intensive assaults. This operational approach reflects Russia's relative advantages in defence-industrial capacity, available manpower reserves and its ability to sustain prolonged high-intensity combat operations.

Russian operations typically rely on the large-scale employment of artillery, rocket forces, thermobaric systems and other long-range fires to suppress, saturate and systematically degrade Ukrainian defensive positions prior to ground assaults. Assault operations are frequently initiated by personnel assessed as lower priority from a force-preservation perspective, including mobilised personnel, irregular formations, recruits from occupied Ukrainian territories, penal units, and contracted foreign personnel. These elements are often employed to probe Ukrainian defensive positions, identify firing points, force the expenditure of ammunition and expose defensive dispositions before the commitment of better-trained and more capable regular units.

From an operational standpoint, this approach enables Russian forces to generate continuous pressure against Ukrainian defensive sectors while preserving higher-value combat formations and experienced personnel for subsequent exploitation or follow-on operations. The practice is also intended to exhaust Ukrainian manpower, ammunition stocks and defensive endurance over time.

As the conflict evolved, Russian operational methods adapted to the realities of resource management, battlefield attrition and the increasing lethality of the modern ISR-strike environment. Large-scale mechanised assaults became less frequent due to their vulnerability to precision fires, anti-armour systems and UAS. Russian forces consequently shifted toward employing smaller, decentralised, and more flexible assault groups, supported by extensive use of reconnaissance and strike drones, loitering munitions, electronic warfare assets, and integrated fire support. This adaptation reflects a broader transition toward dispersed operations designed to reduce vulnerability while maintaining persistent tactical pressure along the frontline. Russia's changing attack tactics are forcing Ukraine to adapt by adopting shorter defence lines and building low-rise strongpoints that are less visible to drones swarming the skies (Melkozerova 2025).

4.2 Ukrainian Defensive Activities

The evolution of the Russia–Ukraine War indicates that Ukraine has progressively shifted towards an attrition-based approach to warfare, seeking to degrade Russian combat power over time by imposing disproportionate losses in personnel, equipment, and combat capability while preserving its own forces. Attrition warfare emphasises the systematic application of firepower to reduce the enemy's fighting capacity rather than achieving decisive results through operational manoeuvre. Consequently, firepower has become the principal means of generating combat effects, whereas manoeuvre primarily serves to create favourable conditions for the employment of fires (Gady 2023).

During the initial stages of the full-scale invasion, Ukraine's operational approach combined defence in depth with elements of mobile defence, enabling Ukrainian forces to absorb Russian offensives before conducting localised counter-offensives and subsequent operational-level offensives in 2023. However, by the end of 2024, Ukraine's ability to sustain large-scale offensive manoeuvre had significantly declined. This resulted from a structural shortage of trained personnel, insufficient stocks of heavy equipment—particularly main battle tanks, infantry fighting vehicles, and other armoured platforms—and the absence of adequate air power to provide effective air support and freedom of manoeuvre. These limitations were further compounded by cumulative combat losses, increasing personnel fatigue, declining morale, and growing difficulties in force generation and regeneration.

The transition towards attrition warfare became particularly evident during 2024 and early 2025, when Ukrainian offensive operations achieved only limited operational gains despite considerable investment in manpower and materiel. At both the tactical and operational levels, extensive Russian defensive fortifications, dense obstacle belts and minefields, persistent artillery superiority, and contested airspace significantly constrained the conduct of combined manoeuvre. Without sufficient fire support, engineering assets, and air superiority—or at least localised air superiority—Ukraine was unable to achieve the tactical success necessary to regain and exploit the operational initiative.

In response to these operational constraints, Ukraine fundamentally adapted its defensive concept at both the operational and tactical levels. Large, readily identifiable defensive positions were progressively replaced by a distributed defensive architecture consisting of multiple mutually supporting trench systems that are dispersed, concealed, and optimised to reduce vulnerability to unmanned aerial systems (UAS). These defensive positions are integrated into a comprehensive network of logistics routes, alternate and supplementary defensive positions, reserve positions, obstacle belts, and minefields, thereby increasing resilience and survivability under persistent Russian reconnaissance and precision fires.

Such an integrated defensive system facilitates sustainment, force rotation, local counterattacks, and, when required, the execution of deliberate withdrawals while preserving combat effectiveness and preventing operational collapse (Melkozerova 2025).

The widespread employment of unmanned systems has become a central component of Ukraine's defensive concept. UAS are routinely employed for ISR, target acquisition, battle damage assessment, artillery fire correction, and precision strike missions. These capabilities enable Ukrainian forces to identify, track, and engage Russian assault formations within pre-designated engagement areas, where concentrated indirect fires can inflict significant losses in personnel and materiel before assault elements reach the main defensive positions. In sectors where operationally and logistically significant urban areas must be defended, urban terrain further enhances the effectiveness of this approach. Urban environments provide favourable conditions for delaying operations, enabling numerically inferior forces to slow Russian advances, impose disproportionate attrition, and gain time for force regeneration, sustainment, and the preparation of successive defensive positions in adjacent sectors, thereby reducing the risk of an operational breakthrough (Spencer 2023).

The cumulative degradation of combat power has increasingly affected both belligerents. Neither the Ukrainian nor the Russian Armed Forces currently demonstrate the capability to conduct sustained large-scale combined offensive operations capable of producing decisive operational breakthroughs. Instead, combat has become increasingly fragmented and localised. This trend is reflected in the reduced scale of tactical action, where the company has increasingly replaced the battalion as the principal tactical manoeuvre element across many sectors of the front. This evolution illustrates the progressive degradation of force structure and combat power, and of both sides' ability to concentrate sufficient forces and capabilities to conduct large-scale offensive operations.

To compensate for its reduced capacity to conduct operational manoeuvre, Ukraine has increasingly relied on long-range precision strike capabilities to generate operational effects beyond the forward line of troops. The introduction of advanced Western systems—including the HIMARS, integrated with ISR support—has significantly enhanced Ukraine's deep-strike capability. Precision engagement of Russian C2 systems, ammunition depots, logistics infrastructure, and other high-value targets has reduced the effectiveness of Russian artillery while complicating Russian sustainment and operational planning. Although these capabilities have improved Ukraine's operational freedom of action, they have not fundamentally altered the overall character of the conflict or restored Ukraine's ability to conduct sustained operational manoeuvre.

Consequently, since early 2024 Ukrainian operations have increasingly combined the principles of attrition warfare with selected elements of manoeuvre warfare. While the overall campaign has remained attrition-based, deep precision strikes have sought to disrupt Russian command and control systems, lines of communication, logistics infrastructure, critical energy facilities, and the physical, functional, and psychological cohesion of Russian forces. These actions have increased the cost of sustaining Russian military operations and reduced the effectiveness of Russian combat support and sustainment systems. However, they have not generated sufficient operational dislocation to restore the conditions necessary for sustained combined offensive operations or to produce decisive operational effects. As a result, Ukraine has remained unable to achieve significant territorial gains or restore the operational momentum required to accomplish its long-term military-strategic objective of liberating occupied territory.

4.3 Long-Range Strike Operations

The employment of long-range fires from within national territory—enabled through a combination of stand-off conventional missile systems and the increasingly widespread use of one-way attack UAS—has attracted considerable attention during the Russia–Ukraine War. In many assessments, these capabilities are presented as a potential model for future force-projection operations. Such conclusions, however, should be treated with caution. The current conflict did not create this operational approach but rather expanded a model of indirect force projection that had already emerged during the previous decade among actors unable to establish air superiority or freedom of action within contested airspace. This approach relies on the coordinated employment of long-range missile strikes and large numbers of relatively low-cost unmanned systems to generate effects against targets located deep within adversary territory.

As such, it represents an alternative means of force projection in environments where conventional air operations are constrained by a robust IAMD architecture. Its effectiveness is therefore inherently linked to the ability of offensive systems to saturate, degrade, or partially neutralise an adversary's IADS when systematic SEAD/DEAD operations are not feasible. The conflict has demonstrated that no air-defence system is entirely impermeable. Even highly sophisticated, layered architectures can be penetrated under specific operational conditions by ballistic, quasi-ballistic, cruise missile, or unmanned threats. Nevertheless, Ukraine has succeeded for much of the conflict in intercepting most of the Russian one-way attack UAS through a combination of Western-supplied air-defence capabilities, adaptive employment concepts, and a comparatively favourable cost-exchange ratio.

Only recently have Russian Aerospace Forces and associated strike forces achieved more significant effects through larger strike packages, increased operational tempo, and evolving employment tactics. Consequently, the long-term viability of this strike model remains closely tied to the ability of defending forces to maintain an acceptable cost-exchange relationship between offensive effectors and defensive interceptors—a challenge of growing relevance for NATO air-defence planning.

Even if air-defence systems are progressively saturated or degraded, the operational effectiveness of long-range strike campaigns remains dependent upon the quality of ISR support. As with traditional air campaigns, target identification, tracking, prioritisation, and battle-damage assessment remain critical prerequisites for achieving operational and strategic effects. In this regard, Ukraine benefits significantly from intelligence support provided by Western partners. However, even when supported by high-quality ISR, current generations of one-way attack UAS generally provide lower destructive effects than manned aircraft employing precision-guided munitions. Their limited payload, lower reliability, and comparatively reduced lethality mean that they cannot yet fully replace cruise missiles, ballistic missiles, or air-delivered precision weapons.

This reality is reflected in Ukraine's continued efforts to acquire advanced Western long-range strike systems and expanded authorisation for their employment. It is similarly evident in the relatively limited military effects achieved by many Russian UAS attacks, which have frequently been employed to generate cumulative pressure on air-defence resources, disrupt civilian activity, and influence public morale rather than produce decisive operational outcomes. At the same time, the relatively limited inventories and high procurement costs of stand-off missile systems constrain their ability to generate effects comparable to those achieved during a comprehensive air campaign.

Current trends suggest that future deep-strike capabilities are likely to evolve along three complementary lines, one of which has been significantly accelerated by lessons from the Russia–Ukraine War: the mass employment of unmanned strike systems. The principal challenge will be increasing their range, survivability, autonomy, payload capacity, and targeting effectiveness while maintaining production costs low enough to enable large-scale employment and favourable cost-exchange ratios. The operational value of these systems will increase further if they can contribute directly to counter-air operations or function as part of a broader strike architecture designed to degrade or suppress elements of an adversary's IADS. This development is closely linked to two additional trends.

The first is the continued evolution of ground-launched long-range strike systems—including ballistic, quasi-ballistic, cruise missile, and hypersonic capabilities—which provide substantial range and kinetic effects against defended targets but are likely to remain relatively scarce due to their high acquisition and sustainment costs.

The second trend involves the development of affordable air-launched stand-off weapons that offer a more economical alternative to traditional cruise missiles while preserving operational reach and precision. Representative examples include ongoing U.S. initiatives focused on affordable mass-effect capabilities, such as the Enterprise Test Vehicle, the Franklin Affordable Mass Missile, and the Extended Range Attack Munition. These programmes seek to combine operational range, precision, survivability, and affordability, thereby enabling the large-scale employment of long-range strike capabilities against adversaries protected by dense and layered air-defence networks.

Taken together, these developments suggest that future force-projection concepts will not replace traditional airpower but will increasingly complement it. The most effective operational approach is likely to involve the integration of manned aviation, stand-off missile systems, unmanned strike platforms, cyber capabilities, electronic warfare, and ISR assets into a comprehensive multi-domain strike architecture capable of generating sustained effects against defended targets across the operational and strategic depth of the battlespace (Trevithick 2024, 2025).

4.4 Air-Surface Integration

Although the conflict has not introduced entirely new operational phenomena, many of the lessons observed correspond to scenarios associated with high-intensity conventional warfare in the Central European theatre that featured prominently in NATO planning during the Cold War. Following the end of the Cold War, however, these considerations were largely superseded by a focus on expeditionary operations and campaigns against adversaries possessing a limited spectrum of military capabilities.

The conflict has reaffirmed the critical importance of EW and its effects on C2 systems, ISR, communications networks, and data transmission systems. It has also highlighted the enduring relevance of EW in supporting the SEAD/DEAD and enabling precision-strike operations. At the same time, the war has extended beyond traditional doctrinal assumptions through the large-scale employment of UAS, a trend previously foreshadowed by conflicts in the Nagorno-Karabakh War and across the Middle East.

One of the most significant operational consequences has been the re-emergence of a predominantly direct approach to warfare, in which firepower rather than manoeuvre increasingly determines battlefield outcomes. The unprecedented transparency of the battlespace, enabled by the widespread availability of low-cost, distributed ISR and strike capabilities—particularly UAS—has significantly reduced forces' ability to conceal, concentrate, and manoeuvre undetected. As a result, hostile forces can be engaged not only along the line of contact but also during force generation, concentration, staging, and deployment activities in the operational rear. This development fundamentally alters traditional operational sequencing and challenges long-standing assumptions regarding the conduct of offensive operations.

The result is the emergence of a form of localised low-altitude air superiority within what U.S. military doctrine has described as the air-land littoral—the battlespace extending from the surface to approximately 1,000 metres above ground level. Control of this zone increasingly depends on the integration of UAS, electronic warfare systems, air-defence assets, and precision fires rather than on conventional manned aviation alone. Consequently, the conflict is reshaping the conduct of combined-arms and joint operations while redefining the requirements for mobility, dispersion, concealment, camouflage, survivability, and passive force protection.

A parallel trend has been the decentralisation of combat capabilities to lower tactical echelons. Battalion- and company-level formations increasingly integrate a high-low mix of ISR assets, indirect fires, ground-based air defence, electronic warfare systems, loitering munitions, and Cyber-Electromagnetic Activities (CEMA) capabilities. Functions previously concentrated at higher headquarters or within specialised units are becoming organic components of tactical formations, thereby increasing responsiveness and shortening sensor-to-shooter timelines.

The Air-Surface Integration represents the domain in which the Russia–Ukraine war has generated some of the most significant transformational effects on the conduct of contemporary military operations. The concept of Air-Surface Integration was born of experience over the past few years and aims to better integrate assets during joint or combined operations to increase the effects of the committed forces. Its application nevertheless calls for both technical and human adaptation (Sutter 2019).

This shift toward a firepower-dominated, highly transparent battlespace represents a significant departure from the Alliance's traditional preference for manoeuvre-centric operations designed to generate rapid operational dislocation and decision advantage.

Under current conditions, the ability to achieve decisive manoeuvre is increasingly constrained, raising the risk that future high-intensity conflicts may evolve into prolonged campaigns of attrition at both the operational and strategic levels. Such a development runs counter to NATO's long-standing emphasis on tempo, operational agility, and decision-centric warfare. Furthermore, the rapid cycles of technological adaptation and counteradaptation observed in Ukraine complicate long-term forecasting of force structures, weapons systems, and tactical procedures. Within the current technological ecosystem, it is increasingly difficult to envisage a battlefield environment in which large-scale force concentrations could be employed without encountering significant operational friction and the potential for tactical stalemate.

Several factors suggest that these observations may be particularly relevant to a potential high-intensity conflict involving NATO and Russia in the Baltic region. The geography of the Baltic-Polish operational area is characterised by extensive forests, wetlands, lakes, and a limited number of major lines of communication, all of which constrain operational manoeuvre and channel movement along predictable avenues of approach. Simultaneously, ongoing defensive preparations—including East Shield and complementary fortification initiatives undertaken by the Baltic states—are likely to increase battlefield compartmentalisation and contribute to a greater degree of linearity in future defensive operations.

In this context, comparisons with the Maginot Line are often misleading. Such assessments frequently overlook that the Maginot Line's failure stemmed primarily from incomplete implementation and inadequate integration into a broader operational concept, rather than from any inherent shortcomings of fortified defensive systems. Indeed, the Russia–Ukraine War has demonstrated that well-prepared defensive belts, fortified positions, obstacle systems, and integrated fires can impose substantial costs on attacking forces. A notable example is the extensive defensive network established by Ukraine in the Donbas region after 2015, which Russian forces penetrated during the 2022–2023 offensive operations, requiring significant expenditures of personnel, materiel, and time. These experiences underscore the continuing operational value of prepared defensive systems when integrated into a comprehensive defensive architecture supported by ISR, fires, engineering assets, and force sustainment capabilities.

4.5 Russian Long-Range Strike Campaign

A further critical dimension of the conflict is the contest between offensive strike operations and infrastructure protection. Russia has conducted a sustained long-range strike campaign employing missiles and one-way attack UAS against Ukrainian critical infrastructure with the objective of degrading Ukraine's war-sustaining capacity, reducing societal resilience, and shaping conditions for subsequent phases of the campaign. Priority targets have included population centres, energy-generation and transmission facilities, and key logistical infrastructure such as power plants, substations, and water distribution networks. Damage to these assets creates a force-multiplying vulnerability by triggering cascading effects across civilian, economic, and military systems (Polishchuk 2025).

The Russian targeting methodology has evolved over time. The campaign has shifted from broad, nationwide attacks on critical infrastructure to more focused efforts targeting specific regional energy generation and transmission nodes, with the objective of overwhelming local capacity and inducing systemic grid failures. Such operations are typically conducted through coordinated employment of large UAS strike packages to saturate air-defence systems and deplete interceptor inventories, followed by precision missile strikes against designated targets.

4.6 Ukrainian Deep-Strike Operations

Ukrainian forces have expanded their deep-strike campaign against military and defence-industrial targets within Russia. These operations target weapons-production facilities, ammunition depots, military bases, command-and-control nodes, and infrastructure supporting hydrocarbon extraction, refining, and transportation. These strikes have targeted oil infrastructure, Russian Naval forces—such as ships docked in Novorossiysk—and the Russian Air Force, for example, striking Shagol airfield in Russia's Chelyabinsk region 1700 km deep into Russia. In the Baltic Sea, these strikes have disrupted oil shipping by repeatedly targeting the ports of Ust-Luga and Primorsk. Ukraine has hit refineries deep inside Russia, including the Tuapse Refinery in Tuapse Region (1,500 km away), the Bashneft-Novoil refinery in Bashkortostan (1,400 km away), and the Novokuybyshevsk Refinery in Samara Region (1,000 km away). In addition, Ukraine has essentially regained control of the Black Sea. They have also struck air defence, radar systems, and other key military infrastructure in Russia and the temporarily occupied territories of Ukraine (Place 2026).

At the same time, Ukraine is constrained by its inability to conduct direct strikes against defence-industrial facilities located within Allied territory or against production capacity that has been dispersed or relocated beyond the Russian Federation's borders. Notwithstanding these limitations, Russia's reliance on large-scale, geographically concentrated defence-industrial complexes creates identifiable and exploitable vulnerabilities within its defence industrial base. As a result, the identification, targeting, and disruption of critical defence-industrial nodes may, under certain conditions, generate favourable cost–effectiveness ratios in terms of operational and strategic effects (Cranny-Evans 2025).

Deep strike operations conducted against Russia's defence-industrial and energy infrastructure have the potential to further degrade its overall military capability. Such effects may compound existing pressures on Russian force generation and sustainment, particularly amid rising personnel losses and declining recruitment. In this regard, continued precision strikes may contribute to the erosion of Russia's battlefield combat power, its capacity to maintain operational tempo, and its ability to generate revenue from the hydrocarbon sector, which remains a key enabler of its war effort. In addition, such operations may reduce Russia's capacity to conduct long-range strikes against Ukrainian civilian infrastructure.

Beyond their physical effects, these operations also generate a significant cognitive and psychological dimension. For years, the Kremlin has sought to project the image of Russia as a geographically vast, strategically insulated, and militarily invulnerable power, largely shielded from the consequences of its own actions. Sustained deep strike activity challenges this narrative by demonstrating the vulnerability of critical nodes within Russia's strategic depth, thereby undermining perceptions of invulnerability and contributing to broader informational and psychological effects.

5. IMPLICATIONS FOR NATO DETERRENCE STRATEGY

The Russia–Ukraine war may represent a similar inflexion point in the evolution of warfare. It highlights significant changes in the conduct of combat operations, particularly at the tactical and operational levels, with direct implications for future capability development and long-term force planning. However, the magnitude of these changes is not uniform across all domains and operational environments. The most visible transformation has occurred within the land and air domains, where advances in ISR, target acquisition, fires integration, force protection and unmanned systems have fundamentally altered how military forces detect, engage and survive against adversaries. The implications for operational manoeuvre, deep operations and force projection remain the subject of ongoing analysis, particularly regarding operations against A2/AD systems, long-range precision strike capabilities and the generation of strategic effects.

The conflict also demonstrates a broader transformation in capability development itself. The rapid proliferation of commercially available technologies, combined with exceptionally short innovation cycles driven by wartime necessity, has challenged traditional defence acquisition processes. Effective military adaptation increasingly depends upon the ability to rapidly identify operational requirements, accelerate experimentation, integrate emerging technologies and field new capabilities at a pace consistent with battlefield developments. This reality reinforces NATO's emphasis on agility, interoperability, innovation and rapid capability insertion as essential requirements for maintaining military effectiveness in future conflicts.

5.1 Technological Advantage in High-Intensity Warfare

The Russia–Ukraine War has demonstrated that technological superiority, while highly advantageous, does not in itself guarantee success in a protracted high-intensity conflict. Advanced weapon systems, precision-guided munitions, sophisticated ISR capabilities, and network-enabled operations can generate significant operational advantages and improve the efficiency of military operations. However, the conflict has also highlighted the limitations of relying exclusively on technological superiority when confronting a capable and resilient adversary in a war of attrition. One of the principal lessons emerging from the war is that the balance between quality and quantity remains a critical consideration in force planning and capability development. Although advanced systems often provide superior battlefield performance, they are frequently expensive, complex to manufacture, and difficult to replace at the rate required during sustained combat operations.

Consequently, the ability to generate mass, regenerate combat power, and sustain operations over time remains a decisive factor in high-intensity warfare. As the conflict in Ukraine illustrates, industrial capacity, production scalability, and logistical resilience are often as important as technological sophistication. In such circumstances, quantity can itself become a source of operational advantage, particularly when supported by effective doctrine, training, and command structures. The conflict further demonstrates that airpower must be employed as an integrated and coherent component of the joint force rather than as a collection of individual platforms or isolated capabilities. The effectiveness of airpower depends upon its ability to generate coordinated effects across multiple domains through the integration of combat aviation, air and missile defence, ISR assets, electronic warfare, space-based capabilities, and increasingly, unmanned systems. Achieving such integration requires appropriate doctrine, effective command-and-control arrangements, and personnel capable of employing airpower in accordance with clearly defined operational objectives. From a NATO perspective, airpower must remain organised and employed according to the principles of centralised control and decentralised execution, allowing scarce and high-value capabilities to be allocated where they can generate the greatest operational effect. Institutional barriers, service rivalries, and legacy organisational approaches that limit the effective employment of air capabilities can reduce operational effectiveness and impede adaptation to evolving battlefield conditions. The experience of Ukraine underscores the importance of doctrinal flexibility, rapid innovation, and the ability to integrate emerging technologies into operational practice.

The war also reinforces the continued importance of deterrence through credible military capability. Effective deterrence depends not only on the possession of advanced military systems but also on the demonstrated ability to employ them at scale and sustain their use over the course of a prolonged conflict. In this regard, NATO's ability to maintain a technologically advanced and resilient European Defence Technological and Industrial Base (EDTIB), supported by robust logistics networks and sufficient production capacity, remains a fundamental component of collective defence. The lessons of the conflict suggest that future deterrence will increasingly depend upon the integration of airpower, long-range precision fires, space-based capabilities, cyber effects, electronic warfare, and missile defence within a coherent multi-domain framework. The objective is not merely to maintain military superiority, but to ensure that any potential adversary understands that aggression against the Alliance would incur unacceptable military, economic, and political costs.

In an increasingly contested strategic environment, the credibility of NATO deterrence will rest on its ability to integrate technological innovation, operational readiness, industrial resilience, and alliance cohesion into a force posture capable of prevailing in a high-intensity conflict against a peer or near-peer adversary. If there is any lesson to be extracted from the Russia-Ukraine war to date, it is the absolute necessity of air superiority to achieve a decisive advantage. Without it, the conflict has devolved into a relative stalemate, literally resembling the trench warfare of the First World War. Neither side has the freedom of manoeuvre and attack that air superiority enables, and victory is likely to go to the side with the most warfighting personnel and materiel—Russia (Deptula 2024).

5.2 NATO–Russia Strategic Competition

By 2025, the Russia–Ukraine War will have evolved beyond a conventional contest for military victory and will increasingly represent a long-term strategic confrontation shaping the future European security architecture. Rather than seeking decisive battlefield outcomes, the principal actors appear focused on managing escalation, preserving strategic leverage, and preventing adverse shifts in the regional balance of power. In this context, the conflict increasingly functions as a framework for strategic competition between NATO and Russia, within which both sides calibrate their actions to avoid either outright defeat or uncontrolled escalation.

This dynamic is reflected in the behaviour of the principal stakeholders. NATO member states continue to provide Ukraine with military, financial, intelligence, and logistical support sufficient to sustain its defence and deny Russia the achievement of its strategic objectives, while carefully managing escalation risks to avoid direct Alliance involvement in the conflict. Russia, for its part, combines sustained military pressure with long-range strike campaigns, nuclear signalling, information operations, and other instruments of state power designed to maintain coercive leverage and strategic influence without crossing thresholds that could trigger a broader confrontation with NATO (Black 2020).

At the strategic level, many of the traditional mechanisms of NATO–Russia dialogue, confidence-building, and security cooperation have largely ceased to function. Nevertheless, neither side has demonstrated a willingness to sever all channels of communication or abandon crisis-management mechanisms entirely. As a result, the absence of a negotiated settlement has itself become a form of strategic equilibrium, characterised by persistent confrontation, controlled escalation, and mutual deterrence.

Within this environment, the central challenge is no longer the achievement of decisive military victory but the management of a protracted strategic competition. NATO and Russia are increasingly adapting their force posture, deterrence strategies, and defence planning processes to a security environment defined by sustained confrontation below the threshold of direct large-scale Alliance–Russia war. The conflict has therefore become not only a struggle over Ukraine's future but also a catalyst for the emergence of a new deterrence-based security order in Europe.

From a NATO perspective, this evolving environment reinforces the importance of credible deterrence and defence, forward-posture forces, military readiness, resilience, and defence-industrial capacity. Simultaneously, Russia continues to pursue a strategy aimed at exhausting Western political cohesion, undermining support for Ukraine, and preserving its ability to influence the regional security architecture. Consequently, the strategic balance emerging in Eastern Europe increasingly resembles a state of managed confrontation in which neither side can impose a decisive outcome, yet both retain sufficient military and political capacity to prevent the other from achieving its objectives.

In this sense, the conflict anticipates a broader transformation of European security. Rather than a return to the traditional post-conflict model based on a formal peace settlement, the emerging order may be characterised by long-term deterrence, persistent competition, and recurring crises managed through calibrated military, political, economic, and informational instruments. The resulting strategic environment is therefore less a transition toward peace than the institutionalisation of a new form of confrontation, in which stability is maintained not through reconciliation but through mutual deterrence and the continuous management of escalation risks.

The following sections examine this evolving strategic equilibrium through two interconnected and mutually reinforcing perspectives. On the one hand, NATO has progressively adapted its approach from immediate crisis response toward a long-term strategy of deterrence, resilience, and the preservation of regional stability. On the other hand, Russia continues to employ military pressure, strategic coercion, information operations, and controlled instability as instruments to constrain Western influence and shape the European security environment to its advantage. The resulting condition is not one of reconciliation or strategic convergence, but rather a form of managed confrontation characterised by persistent competition below the threshold of direct NATO–Russia conflict. This emerging reality—deterrence without decisive victory—has become a defining feature of European security in 2025 and provides important insights into the future evolution of the continent's strategic order.

5.3 Adaptive Approach to NATO Deterrence Strategy

By 2025, NATO's deterrence and defence posture represents the culmination of a decade-long process of strategic adaptation initiated in response to Russia's annexation of Crimea in 2014. This evolution is firmly anchored in the 2022 Strategic Concept, which outlines the security environment facing the Alliance, reaffirms its fundamental values, and defines NATO's primary purpose: ensuring collective defence for all Allies. The NATO 2022 Strategic Concept also establishes NATO's three core tasks—deterrence and defence, crisis prevention and management, and cooperative security—which collectively provide the strategic framework for the Alliance's ongoing adaptation to an increasingly complex and contested security environment (NATO 2022). Within this framework, the adoption of the Readiness Action Plan (RAP) marked the beginning of a transition from reassurance measures toward a more robust forward defence posture along the Alliance's eastern flank. Over time, NATO has evolved from a model primarily focused on crisis response and assurance to one centred on persistent deterrence and collective defence. This transformation is reflected in the progression from the Enhanced Forward Presence (eFP) and Tailored Forward Presence (tFP) initiatives to the broader concept of Deterrence and Defence of the Euro-Atlantic Area (DDA) (NATO 2025a).

The DDA concept, formally endorsed in 2020 and further operationalised through NATO's new regional defence plans approved at the 2023 Vilnius Summit and implemented thereafter, constitutes the foundation of the Alliance's contemporary deterrence architecture. It integrates conventional and nuclear deterrence, IAMD, cyber defence, space-based capabilities, civil preparedness, and societal resilience within a coherent, multi-domain framework. The objective is to provide a credible and scalable deterrence posture capable of addressing a broad spectrum of threats while maintaining escalation control and preserving Alliance cohesion.

This approach reflects NATO's emphasis on integrated deterrence, whereby military capabilities are synchronised with political, economic, technological, and informational instruments of power. The Alliance seeks to ensure that deterrence remains visible, credible, and sustainable without generating unnecessary risks of escalation. Consequently, deterrence is no longer viewed solely through the lens of force posture and military presence, but as a comprehensive effort to strengthen resilience, enhance readiness, and reduce strategic vulnerabilities across the Euro-Atlantic area. In this respect, the principles articulated in the NATO 2022 Strategic Concept have provided the conceptual foundation for a more integrated and multidimensional approach to deterrence and defence.

Forward defence remains a central component of this strategy. Multinational formations deployed under the eFP and tFP frameworks in Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Romania, and Bulgaria form the forward element of NATO's deterrence posture. These forces are increasingly integrated into a broader operational architecture that links the Arctic and the High North, the Baltic region, Central Europe, and the Black Sea into a single strategic area.[14] Supported by pre-positioned equipment, improved military mobility, enhanced command-and-control arrangements, and regularly exercised reinforcement plans, these formations provide both a deterrent signal and an initial defensive capability.

The implementation of NATO's regional plans has further strengthened interoperability and responsiveness across the Alliance. Forward-deployed multinational formations are now integrated into more agile command structures, supported by high-readiness forces, strategic enablers, and increasingly resilient logistics networks. The ability to rapidly reinforce threatened sectors has become a critical component of deterrence by denial, with key European Allies playing an important role in sustaining military mobility, host-nation support, strategic transportation, and rear-area logistics. As a result, NATO's deterrence posture in 2025 can be characterised as a multi-domain, theatre-wide, and networked system of deterrence and defence extending from the Arctic and High North through the Baltic region to the Black Sea. Rather than relying solely on forward troop deployments, the Alliance increasingly emphasises integrating combat-ready forces, resilient logistics, MDO capabilities, and collective decision-making mechanisms. This adaptive posture is designed to deter aggression, ensure freedom of action for Allied forces, and preserve the stability of the Euro-Atlantic security environment in an era of sustained strategic competition.

A particularly significant element of NATO's evolving deterrence and defence posture is the implementation of the NATO Regional Defence Plans. At the 2022 NATO Summit in Madrid, Allies agreed to establish the New NATO Force Model (NFM) as a central component of the Alliance's strengthened deterrence and defence posture. The NFM replaced the former 40,000-strong NATO Response Force (NRF) and was designed to provide a substantially larger pool of forces available for rapid deployment during crises.

[14] Within the NATO military command structure, the Supreme Allied Commander Europe (SACEUR) is responsible for the overall planning and command of NATO military operations. The SACEUR Area of Responsibility (AOR) encompasses all NATO operations across the Euro-Atlantic region, including the territories of all member states in North America and Europe, as well as the Atlantic Ocean and the Mediterranean Sea.

Unlike the NRF, which maintained a readiness level of approximately 15 days, the NFM is structured around three readiness tiers, enabling deployment of forces within 10 to 180 days. The model also laid the foundation for implementing NATO's Regional Defence Plans by pre-assigning forces to specific operational requirements and providing the high-readiness capabilities necessary to establish the Allied Reaction Force (ARF).

This development represents not only a military adaptation but also a strategic and political transformation. NATO's approach increasingly emphasises deterrence through integration, resilience, and collective defence rather than reliance on direct military confrontation. The objective is to deny potential adversaries opportunities to exploit regional vulnerabilities by creating a highly interconnected security architecture that enables rapid, coordinated responses across multiple domains (Bryan 2025).

Within this framework, the United States remains the Alliance's principal strategic enabler and the ultimate guarantor of extended deterrence. U.S. capabilities—including strategic ISR, IAMD, strategic lift, advanced C2 systems, long-range precision strike capabilities, and globally deployable air and maritime forces—continue to underpin the credibility of NATO deterrence and defence. Washington plays a central role in maintaining Alliance cohesion, calibrating deterrence measures, managing escalation risks, and ensuring the operational integration of multinational formations and regional defence plans.

By 2025, U.S. strategy increasingly reflects a dual objective: sustaining support for Ukraine and reinforcing NATO's eastern flank while avoiding direct military confrontation with Russia. At the same time, the United States continues to encourage greater European responsibility for regional security. This approach is particularly evident in the implementation of NATO's Regional Defence Plans, where European Allies are assuming a larger role in force generation, military mobility, logistics, and the defence of key operational theatres such as the Baltic and Black Sea regions. Rather than reducing its commitment to European security, the United States is pursuing a more balanced model of burden sharing that combines sustained American strategic leadership with increased European contributions to collective defence.

5.3.1 Sustainability and Resilience of NATO Deterrence Posture

The current security environment demonstrates that, despite significant progress in defence spending, force readiness, and the integration of Finland and Sweden into the Alliance's defence architecture, NATO continues to face significant challenges in defence-industrial capacity, military mobility, logistics, and force sustainment. The central objective is no longer merely to demonstrate the Alliance's ability to respond rapidly to crises, but to institutionalise a credible and enduring deterrence posture capable of maintaining strategic stability through continuous planning, interoperability, readiness, and strategic communication.

Within this framework, sustainability has emerged as a critical component of NATO's deterrence and defence posture. Effective deterrence requires not only combat-ready forces but also the capacity to sustain military operations, regenerate combat power, replenish critical stockpiles, and maintain political cohesion over extended periods of strategic competition. The experience of the Russia–Ukraine War has demonstrated that long-term military effectiveness depends as much on industrial resilience, logistics, and societal endurance as on the capabilities of deployed forces.

The defence industry has therefore assumed increasing importance within Allied planning. Initiatives aimed at strengthening EDTIB, expanding production capacity, and enhancing interoperability among Allied defence industries seek to ensure that military capabilities can be generated, sustained, and regenerated at a pace consistent with the demands of high-intensity warfare. The strategic objective is not the indefinite expansion of force structures, but rather the creation of resilient force-generation systems capable of replacing losses, replenishing stocks, and sustaining operational readiness throughout a prolonged crisis or conflict.

The lessons of Ukraine have reinforced the understanding that deterrence must be conceived as a long-term condition rather than a temporary response to a specific crisis. As a result, NATO is increasingly focusing on integrating defence planning, capability development, industrial production, logistics, and strategic communication into a coherent deterrence framework. The credibility of deterrence is progressively linked to the Alliance's ability to adapt continuously to evolving threats while maintaining unity of effort across the military, political, economic, and industrial areas. In this context, the management of strategic endurance has become a central challenge. Military readiness, industrial output, public support, and political cohesion must all be sustained over time despite the pressures associated with prolonged strategic competition.

Consequently, deterrence is increasingly viewed as a process of continuous calibration rather than one of constant escalation. Maintaining credibility does not necessarily require the continuous escalation of military pressure; rather, it requires the ability to adjust force posture, capability development, industrial production, and strategic messaging in ways that preserve both effectiveness and sustainability.

From a NATO perspective, sustainable deterrence can therefore be understood as a dynamic equilibrium that balances military capability with long-term resilience, deterrence requirements with political cohesion, and operational readiness with industrial capacity. Stability is no longer regarded as a fixed end state but as an ongoing process requiring constant adaptation and management.

While NATO seeks to preserve security through an integrated framework of deterrence, resilience, and collective defence, Russia continues to pursue a contrasting approach that leverages strategic uncertainty, coercion, and controlled instability as instruments of state power. The interaction between these competing approaches increasingly defines the security environment in Europe and the broader trajectory of NATO–Russia strategic competition.

5.4 Russian Strategic Adaptation and Competitive Containment

According to several Western assessments, Russian strategic culture does not view war as an exceptional condition but rather as a continuation of long-term geopolitical competition. From this perspective, military operations constitute one element within a broader framework of state power that integrates military, economic, political, informational, and societal instruments to achieve strategic objectives. The Russia–Ukraine War has reinforced this approach, demonstrating Russia's emphasis on endurance, resilience, and the ability to sustain prolonged confrontation with the West rather than achieving rapid and decisive military victory.

Within this framework, Russian military adaptation is closely linked to the state's capacity to absorb political, economic, and military pressures while maintaining strategic freedom of action. The resilience of the defence-industrial base, the mobilisation of national resources, and the maintenance of domestic political stability form mutually reinforcing pillars of Russia's warfighting capacity. Rather than focusing exclusively on battlefield success, Russian strategy increasingly seeks to sustain a favourable balance of strategic endurance by preserving combat power, maintaining force generation capacity, and outlasting the political will of its adversaries.

Military reforms initiated after 2008 have contributed to the development of a force structure designed for sustained, multi-domain confrontation. Russian military capabilities increasingly integrate long-range precision strike systems, EW, cyber capabilities, information operations, unmanned systems, and conventional manoeuvre forces within a unified operational framework. The expansion of defence-industrial production, the accumulation of strategic reserves, and the continued generation of personnel through mobilisation and recruitment mechanisms have enabled Russia to sustain combat operations despite significant battlefield losses and international sanctions.

In operational terms, Russia has adopted an incremental and calibrated approach to strategic competition. Military pressure is applied continuously but generally below thresholds likely to trigger direct NATO military intervention. This approach seeks to impose cumulative costs, exploit perceived vulnerabilities, and test the cohesion, endurance, and decision-making processes of Western governments and institutions. The objective is not necessarily to achieve rapid escalation, but rather to maintain persistent pressure that gradually shapes the strategic environment in Russia's favour (Edwards 2025).

This strategy extends beyond the battlefield and incorporates a broad range of non-kinetic instruments. Information operations, cyber activities, political influence campaigns, economic leverage, and strategic messaging remain central components of Russian statecraft. Such activities seek to influence public perceptions, undermine confidence in Western institutions, exacerbate political divisions, and complicate collective decision-making processes within NATO and the European Union.

Long-range strike campaigns against Ukrainian critical infrastructure represent another manifestation of this approach. Attacks against energy-generation facilities, transmission networks, transportation infrastructure, and other critical systems aim not only to degrade Ukraine's war-sustaining capacity but also to impose cumulative economic and societal costs over time. These operations reflect a broader strategy of strategic attrition designed to weaken an opponent's capacity and willingness to sustain prolonged resistance.

At the strategic level, Russia continues to employ nuclear signalling as an instrument of deterrence and coercion. Through periodic references to its nuclear capabilities and strategic forces, Moscow seeks to influence Western risk calculations, constrain escalation dynamics, and reinforce perceptions of the potential costs of deeper involvement in the conflict. While these actions generally remain below the threshold of direct nuclear coercion, they form part of a broader effort to shape the decision-making environment and preserve strategic ambiguity (Idarand 2025).

Consequently, Russia’s contemporary approach can be characterised as a strategy of competitive containment based on endurance, adaptation, and controlled escalation. Rather than seeking decisive confrontation with NATO, Moscow appears focused on sustaining a long-term strategic competition in which military power, economic resilience, information influence, and political endurance are employed in combination to preserve Russia’s position within the evolving European security order (Luzin 2025). In contrast to NATO’s emphasis on deterrence through resilience, integration, and collective defence, Russia continues to leverage uncertainty, coercive pressure, and managed instability as instruments to shape the strategic environment and constrain its adversaries' actions.

A notable illustration of Russia’s strategic signalling approach was President Vladimir Putin’s direct participation in a strategic nuclear forces exercise conducted in late 2025, shortly after the postponement of a planned high-level meeting with Donald Trump. Widely publicised by Russian state media and accompanied by large-scale strategic-force activities, the event appeared intended primarily as a demonstration of strategic resolve and nuclear credibility rather than as preparation for immediate military employment.

Such actions reflect Russia’s continuing emphasis on strategic signalling designed to reinforce deterrence, demonstrate great-power status, and communicate escalation thresholds without crossing them. The foundations of this approach predate the full-scale invasion of Ukraine and are rooted in a long-standing Russian strategic culture that places considerable emphasis on resilience, sovereignty, and resistance to external pressure. Within this framework, the state's ability to withstand political, economic, and military challenges is often portrayed as a measure of national strength and legitimacy. Strategic endurance is therefore viewed not merely as a military requirement but as a fundamental component of national security and state continuity.

This perspective is reinforced by Russia’s enduring perception of strategic competition with the West as a long-term, multidimensional contest that extends beyond the military domain. Political, economic, informational, cultural, and technological factors are regarded as interconnected elements of national power. Consequently, measures that might be viewed externally as costly—such as sanctions, economic restrictions, or prolonged military commitments—are often framed domestically as evidence of national resilience and strategic autonomy.

The defence-industrial sector plays a central role within this model. Since 2022, Russia has significantly expanded defence production, increased military expenditure, and reoriented substantial segments of its industrial base toward supporting long-term military requirements.

The resulting capacity to generate ammunition, weapons systems, and military equipment at scale has become a critical enabler of sustained combat operations. In strategic terms, industrial resilience functions not only as a source of combat power but also as a component of deterrence, signalling Russia's ability to absorb losses and sustain prolonged confrontation.

Against this backdrop, Russia's contemporary foreign and security policy exhibits a revisionist dimension aimed less at overturning the international system than at resisting the expansion of political and security arrangements perceived as detrimental to Russian interests. From Moscow's perspective, strategic competition is therefore centred on preserving freedom of action, maintaining spheres of influence, and preventing the emergence of security architectures that could constrain Russia's geopolitical position (Sakwa 2017).

Within this framework, deterrence assumes a broader meaning than its traditional military interpretation. Conventional forces, strategic nuclear capabilities, information operations, cyber activities, and economic instruments collectively contribute to a multi-domain deterrence posture intended to shape adversary decision-making, impose strategic caution, and protect Russia's perceived core interests. Rather than seeking decisive victory through direct confrontation, this approach aims to increase the costs, risks, and uncertainties associated with policies viewed as adverse to Russian objectives. Russia's growing cooperation with partners such as China, Iran, and North Korea further supports this strategy by enhancing its industrial capacity, access to technology, diplomatic flexibility, and strategic resilience. These relationships contribute to Moscow's ability to mitigate external pressures and sustain long-term competition despite economic sanctions and international isolation efforts.

As a result, the ongoing confrontation between Russia and the West increasingly resembles a condition of persistent strategic competition rather than a conflict oriented toward decisive resolution. From Moscow's perspective, the objective is not necessarily to secure an outright victory but to prevent adversaries from achieving their strategic goals, to constrain their freedom of action, and to preserve Russia's position within the evolving European security architecture. In this environment, deterrence becomes a continuous and multidimensional instrument of statecraft, while strategic attrition, resilience, and endurance serve as key mechanisms through which Russia seeks to shape the long-term balance of power in Europe.

5.5 Fragile Strategic Equilibrium and Risk of Competition

The strategic equilibrium between NATO and Russia in 2025 is not the product of temporary political choices but rather reflects the enduring dynamics of international security competition. In an international system characterised by the absence of a supranational authority capable of guaranteeing security, states remain ultimately responsible for their own survival and defence (Waltz 1979). Consequently, both NATO and Russia continue to pursue policies designed to enhance their security, resilience, and strategic freedom of action. This dynamic generates a persistent security dilemma in which measures intended to strengthen deterrence and defence by one actor are frequently perceived by the other as potential threats, thereby stimulating reciprocal adaptation and balancing behaviour.

Within this framework, NATO has progressively refined its deterrence and defence posture to counter potential Russian military advantages while preserving strategic stability and preventing uncontrolled escalation.

Conversely, Russia seeks to offset what it perceives as NATO's superior aggregate military, economic, and technological capabilities through a combination of military modernisation, strategic signalling, information activities, and calibrated coercive measures. The resulting balance is therefore shaped less by political goodwill than by the interaction of competing security interests and mutual perceptions of vulnerability (Mearsheimer 2001). This strategic competition has produced a relatively stable, albeit fragile, deterrence environment. Both sides continue to strengthen their military capabilities and readiness levels, not necessarily to prepare for imminent conflict, but to reduce perceived vulnerabilities and enhance their ability to deter coercion. Within this context, Ukraine remains a central element of the broader NATO–Russia confrontation, functioning simultaneously as an active theatre of conflict, a strategic buffer, and a focal point for competing visions of the European security order.

NATO's DDA concept provides the principal framework for Allied deterrence and collective defence. The DDA integrates conventional forces, nuclear deterrence, cyber defence, space capabilities, strategic communications, civil preparedness, and defence-industrial resilience into a coherent, multi-domain architecture. The objective is to ensure credible deterrence across the full spectrum of conflict while maintaining Alliance cohesion and control of escalation. Large-scale multinational exercises continue to play a critical role in demonstrating readiness, validating regional defence plans, and enhancing interoperability among Allied forces. Operation Eastern Sentry, conducted across NATO's eastern flank, reinforces collective defence commitments and improves the Alliance's ability to rapidly reinforce threatened regions (SHAPE/ACO 2025).

Similarly, exercise Steadfast Noon 2025, NATO's annual nuclear deterrence exercise, validated the readiness, interoperability, and credibility of the Alliance's nuclear deterrence posture. NATO's nuclear forces continue to constitute a core element of the Alliance's deterrence and defence architecture, underpinning collective security while supporting strategic stability through restraint, transparency, and effective escalation management (NATO 2025b).

Russia, meanwhile, continues to employ a combination of conventional military activities, strategic messaging, information operations, cyber capabilities, and demonstrations of military readiness to signal resolve and maintain strategic pressure. Military exercises conducted jointly with Belarus, long-range strike demonstrations, and various forms of strategic signalling are designed to reinforce deterrence, shape adversary perceptions, and preserve strategic ambiguity without necessarily crossing thresholds that could trigger direct confrontation with NATO.

Contemporary deterrence increasingly depends not only on military capabilities but also on perception management and strategic communication. The credibility of deterrence is influenced by an adversary's assessment of political will, Alliance cohesion, military readiness, and the capacity to sustain operations over time. Consequently, signalling unity, resolve, and preparedness has become as important as the deployment of forces themselves. The principal risks to European security, therefore, stem less from deliberate aggression than from the possibility of miscalculation, unintended escalation, or strategic misunderstanding within a context of prolonged competition. Both NATO and Russia continue to operate in proximity across multiple domains, increasing the importance of crisis-management mechanisms, communication channels, and escalation-control measures. Geographically, the strategic centre of gravity of Allied deterrence has expanded significantly since Finland and Sweden joined NATO. The Alliance's northern flank has become a critical component of regional defence planning, while enhanced integration across the Baltic Sea, Nordic region, and Black Sea has contributed to the creation of a continuous deterrence and defence architecture stretching from the High North to Southeastern Europe. This integrated posture reduces opportunities for strategic surprise and complicates potential adversary planning (Vanaga 2019).

At the operational level, the credibility of deterrence increasingly depends on sustainability rather than short-term force generation. The ability to sustain military operations, replenish stockpiles, regenerate combat power, and maintain political cohesion over extended periods has emerged as a decisive factor in strategic competition.

The lessons of the Russia–Ukraine War have reinforced the importance of logistics, military mobility, defence-industrial capacity, and societal resilience as critical enablers of long-term deterrence. The cognitive dimensions and industrial factors further reinforce this evolving deterrence framework. Information operations, strategic narratives, and influence activities have become integral elements of contemporary competition, as public perception, societal resilience, and political cohesion directly affect the credibility of deterrence. At the same time, European efforts to strengthen the EDTIB seek to increase production capacity, interoperability, and strategic autonomy. Initiatives aimed at expanding ammunition production, improving military mobility, enhancing integrated air and missile defence, and deploying cost-effective surveillance and unmanned systems along NATO's eastern flank illustrate this broader trend (European Commision 2025).

Consequently, deterrence in 2025 extends far beyond the traditional threat of military retaliation. It increasingly rests on the capacity to endure, adapt, and sustain strategic competition over time. Military capability, industrial resilience, societal cohesion, and political unity collectively form the foundation of a strategic equilibrium that seeks not to achieve decisive victory but to prevent coercion, manage risks, and preserve stability in an increasingly contested European security environment (EEAS 2025).

The strategic equilibrium between NATO and Russia is shaped by a complex interaction of military, political, economic, technological, and cognitive factors. The principal elements influencing this balance in 2025 are summarised in Table 8.

Table 8: Key Factors Shaping the NATO - Russia Strategic Balance in 2025 (Author)

Factor	NATO Approach	Russian Approach	Impact on Strategic Balance
Deterrence Strategy	Integrated Deterrence and Defence (DDA), combining conventional, nuclear, cyber, space, and resilience capabilities.	Comprehensive deterrence based on conventional, nuclear, informational, economic, and coercive instruments.	Creates a condition of mutual deterrence and strategic competition.
Military Readiness and Force Posture	Enhanced Forward Presence, regional defence plans, New NATO Force Model, high-readiness forces.	Force generation through mobilisation, military modernisation, and maintenance of strategic reserves.	Reduces opportunities for strategic surprise and strengthens crisis response capabilities.
Nuclear Deterrence	U.S. extended deterrence, supported by Allied nuclear-sharing arrangements and strategic forces.	Strategic and non-strategic nuclear capabilities supported by deliberate ambiguity.	Maintains strategic stability while increasing the risk of escalation.
Conventional Military Capability	Superior aggregate military, economic, and technological resources.	Emphasis on mass, force regeneration, long-range strike systems, and attritional warfare.	Produces a balance between NATO's qualitative advantages and Russia's capacity for sustained warfare.
Defence Industrial Capacity	Expansion of the European Defence Technological and Industrial Base (EDTIB), increased ammunition production, and rearmament.	Wartime industrial mobilisation and expansion of defence production.	Industrial resilience increasingly determines the credibility of long-term deterrence.
Political Cohesion and Strategic Will	Alliance cohesion, collective defence commitments, and political solidarity among Allies.	Centralised decision-making and long-term strategic endurance.	Political unity becomes a critical determinant of deterrence effectiveness.
Information and Cognitive Dimensions	Strategic communications, public diplomacy, and counter-disinformation efforts.	Information operations, strategic narratives, influence campaigns, and perception management.	Shapes public perceptions, political decision-making, and deterrence credibility.
Cyber and Hybrid Activities	Enhanced cyber defence, resilience, and protection of critical infrastructure.	Cyber operations, information activities, economic pressure, and hybrid tactics.	Sustains competition below the threshold of armed conflict.
Geography and Strategic Positioning	Strengthened northern and eastern flanks following the accession of Finland and Sweden; integrated defence from the High North to the Black Sea.	Strategic pressure along NATO's periphery through Belarus, Kaliningrad, the Arctic, and the Black Sea region.	Alters regional military balances and reinforces deterrence requirements.
Sustainability and Resilience	Focus on logistics, military mobility, stockpile replenishment, societal resilience, and long-term sustainment.	Reliance on strategic endurance, economic adaptation, and mobilisation mechanisms.	Long-term sustainability increasingly outweighs short-term battlefield success.
Strategic Ambiguity and Escalation Management	Emphasis on transparency, clearly communicated deterrence commitments, and escalation control.	Deliberate ambiguity regarding escalation thresholds and potential use of force.	Increases uncertainty and raises the risk of miscalculation.
Role of Ukraine	Support for Ukraine as a means of strengthening European security and constraining Russian aggression.	Seeks to prevent Ukraine’s integration into Western security structures and maintain strategic influence.	Ukraine remains the principal focal point of NATO–Russia strategic competition.

5.6 Strategy of Deterrence as the Key Principle of European Defence

By 2025, the Russia–Ukraine War no longer represents an isolated crisis but has evolved into the principal framework through which NATO and Russia conduct and regulate their broader strategic competition. Deterrence has emerged as the dominant organising principle of this confrontation, providing the mechanism through which both actors assess relative power, resilience, and strategic credibility while avoiding direct large-scale confrontation. Rather than pursuing decisive military victory, both sides increasingly focus on preventing the other from achieving strategic success.

NATO has progressively consolidated a long-term deterrence and defence posture through the implementation of regional defence plans, enhanced forward presence, strengthened force readiness, and substantial investments in defence-industrial capacity. These measures are designed to deny Russia potential strategic advantages, reinforce Alliance cohesion, and ensure the ability to sustain collective defence over an extended period. The Alliance's approach reflects a comprehensive understanding of deterrence, integrating military capabilities, industrial resilience, societal preparedness, and political unity into a coherent strategic framework.

Russia, for its part, has institutionalised a strategy centred on strategic endurance and competitive pressure. This approach combines defence-industrial expansion, force generation through mobilisation mechanisms, long-range strike capabilities, information operations, energy leverage, and the exploitation of regional instability to sustain pressure on its adversaries. Rather than seeking to reconstruct the European security order on entirely new foundations, Moscow appears primarily focused on preventing the consolidation of a Western-led security architecture that it perceives as detrimental to its strategic interests (Engelbrekt Bakardjieva 2024).

The resulting strategic environment is characterised by a state of mutual deterrence that discourages either side from pursuing actions likely to lead to uncontrolled escalation. Stability is therefore not founded upon political agreement or conflict resolution but upon a balance of competing capabilities, vulnerabilities, and risk calculations. This equilibrium represents a form of strategic stalemate in which both actors seek to preserve their positions while limiting their adversary's opportunities to decisively alter the existing balance.

As the conflict has evolved, the centre of gravity has progressively expanded beyond the battlefield to encompass defence-industrial capacity, technological innovation, political cohesion, societal resilience, and strategic communication. Consequently, deterrence increasingly depends on the ability to sustain long-term competition across military and non-military domains while preventing uncontrolled escalation.

The Russia–Ukraine War demonstrates that deterrence has become the principal organising principle of European security. Strategic stability is increasingly maintained through credible deterrence, resilience, and the ability to manage prolonged strategic competition rather than through political settlement alone (Greminger 2022).

This equilibrium remains inherently fragile, yet it has proven sustainable. It is likely to persist as long as neither NATO nor Russia possesses the capability, political will, or strategic incentive to replace deterrence with a decisive political settlement or military outcome. In this sense, deterrence has evolved from a temporary instrument of crisis management into the central mechanism governing European security and strategic stability in the contemporary era.

5.6.1 Nuclear Deterrence and European Defence

The Russia–Ukraine War has, without a doubt, extremely significant implications for the European nuclear deterrence architecture. These developments should be understood within the broader context of NATO's deterrence and defence strategy, in which nuclear deterrence remains a crucial component of the Alliance's collective defence. While credible conventional forces, resilience, and multi-domain capabilities should constitute the foundation of future deterrence, the conflict has reaffirmed the enduring role of nuclear deterrence in preventing strategic escalation, preserving Alliance credibility, and underpinning Euro-Atlantic security in an increasingly contested strategic environment.

The conflict has reinforced concerns regarding long-term strategic stability and has stimulated renewed debate on the role of nuclear deterrence within the broader European security framework. In several Central and Eastern European countries, particularly in Poland, public and political discussions concerning national security have increasingly included questions about nuclear deterrence. At the same time, greater attention has been directed toward the role of France, the only nuclear-weapon state within the European Union, and to French proposals aimed at initiating a broader European dialogue on the future of nuclear deterrence. Although the establishment of a genuinely European nuclear umbrella remains politically and strategically complex, the re-emergence of this debate reflects the depth of the strategic changes currently affecting the European security environment (Sorg 2025).

These developments are closely linked to concerns about the long-term credibility and sustainability of the United States extended nuclear deterrence, particularly amid evolving geopolitical priorities and growing uncertainty in the international security environment. As a result, questions surrounding the future balance between transatlantic security guarantees and European strategic responsibility have become increasingly prominent. This trend has the potential to place additional pressure on the global nuclear non-proliferation regime while simultaneously reinforcing the role of nuclear deterrence as a central component of European security and defence policy.

Within this context, a growing strategic debate has emerged concerning the relationship between Europe's continued reliance on NATO's nuclear deterrence posture and broader ambitions for greater European strategic autonomy. Attention has been devoted to assessing whether a more Europeanized deterrence framework could complement existing transatlantic arrangements while preserving Alliance cohesion and maintaining credible deterrence against potential adversaries. Consequently, the question is no longer whether nuclear deterrence remains relevant to European security, but rather how to adapt it to support both collective defence and long-term strategic stability in an increasingly contested security environment (Sorg 2025).

5.6.2 Russian Deterrence Strategy Style - Coercion and Strategic Ambiguity

The Russia–Ukraine War has served as a critical test of Russia's deterrence posture, revealing both the strengths and limitations of Moscow's approach to integrating conventional, nuclear, informational, and non-military instruments of power. The employment of dual-capable delivery systems, long-range precision-strike weapons, and strategic messaging campaigns has demonstrated Russia's intent to employ military capabilities not only for operational effects but also for coercive signalling and strategic influence. At the same time, the conflict has exposed limitations within Russia's conventional military instrument, particularly in achieving decisive operational outcomes against a determined adversary supported by extensive Western military assistance and increasingly capable integrated air and missile defence systems (Kaushal 2025).

The war has consequently compelled Russian policymakers and military leaders to reassess the survivability, effectiveness, and sustainability of key strategic capabilities, as well as the viability of maintaining escalation dominance—the ability to control the intensity and trajectory of a regional conflict while deterring adversary escalation (Kofman 2020b).

Rather than relying exclusively on military superiority, Russian strategy increasingly seeks to combine military and non-military instruments in a comprehensive coercive framework designed to shape adversary behaviour and strategic decision-making.

A central component of this approach is the concept often described as cross-domain coercion. Within this framework, deterrence extends beyond the threat of military force and incorporates measures intended to influence perceptions, complicate decision-making processes, and affect political will. Conventional forces, nuclear capabilities, cyber operations, information activities, economic instruments, and diplomatic signalling are employed in a coordinated manner to create uncertainty and impose strategic costs on an opponent. The objective is not necessarily to achieve decisive military victory but rather to shape the adversary's calculations while preserving freedom of action and strategic initiative. In this context, military power is exercised as much through perception management and strategic ambiguity as through the direct application of force. The apparent inconsistency of Russia's nuclear posture should therefore be understood less as evidence of institutional dysfunction and more as a deliberate component of its deterrence strategy (Eken 2025).

Official statements concerning potential escalation pathways, together with strategic messaging, deception and distortion, are accompanied by differing interpretations of the role and potential use of non-strategic nuclear weapons. Some Russian analysts advocate the potential use of non-strategic nuclear warheads delivered by tactical systems, while others emphasise strategic delivery platforms or a sole reliance on strategic nuclear forces (Adamsky 2024). This absence of a single, clearly defined doctrinal interpretation contributes to uncertainty regarding Russian escalation thresholds and decision-making processes, thereby enhancing the deterrent value of the posture itself.

Historical factors have reinforced this ambiguity. The Presidential Nuclear Initiatives (PNIs) of 1991–1992, implemented as unilateral political measures rather than legally binding arms-control agreements, preserved significant flexibility regarding Russia's non-strategic nuclear arsenal and its potential employment concepts (Eli 2004). Consequently, Russian strategic culture has retained substantial latitude in interpreting the role of nuclear weapons within broader deterrence and coercion strategies.

The resulting ambiguity is compounded by the absence of publicly articulated, highly specific escalation criteria, thereby providing Russian political and military leadership with considerable discretion in crisis situations. Similarly, the so-called "Gerasimov Doctrine," frequently referenced in Western commentary as a formal doctrine of Russian hybrid warfare, is better understood as a descriptive label for evolving Russian strategic thought rather than an official doctrinal document.

As noted by Galeotti, the concept reflects the adaptive and often fluid nature of Russian approaches to contemporary conflict rather than a codified strategy (Galeotti 2018).

The revision of Russia's Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence in 2024 further reinforces the central role of ambiguity within Russian deterrence policy. The updated document broadens the scope of actors potentially subject to nuclear deterrence measures, extending beyond nuclear-armed states to include non-nuclear states that Moscow assesses as facilitating or enabling military actions against the Russian Federation. This includes states providing territory, airspace, infrastructure, or other forms of support for hostile operations, as well as military alliances whose members participate in such activities. Nuclear deterrence is therefore increasingly framed not solely as a military instrument but also as a political and psychological mechanism intended to influence the behaviour of both direct and indirect adversaries before a crisis escalates into armed confrontation.

From this perspective, ambiguity constitutes a deliberate feature rather than a weakness of Russian deterrence strategy. Strategic uncertainty complicates adversary planning, increases perceived escalation risks, and enhances Russia's ability to influence decision-making without necessarily resorting to military action. For European states and NATO, understanding this dynamic is essential. The development of a credible and resilient deterrence posture requires not only adequate military capabilities but also a clear appreciation of how Russia employs ambiguity, signalling, and uncertainty as integral components of its broader strategy. Effective deterrence will therefore depend upon the Alliance's ability to establish clear thresholds, maintain strategic coherence, and develop response mechanisms capable of operating effectively within an environment characterised by persistent uncertainty and calibrated coercion.

5.6.3 Dilemma for Europe - Strategic Autonomy and Nuclear Security

The debate on the future of European nuclear security represents a natural extension of broader discussions concerning deterrence, collective defence, and strategic autonomy. The evolving security environment created by the Russia–Ukraine War has intensified consideration of how Europe can strengthen its contribution to deterrence while remaining firmly anchored within the transatlantic security architecture. This discussion inevitably requires an assessment of France's role as the European Union's sole nuclear-weapon state, as well as an examination of potential forms of European cooperation that could enhance deterrence while remaining consistent with international non-proliferation commitments and broader strategic stability. Within this context, proposals concerning a potential European deterrence capability—although still largely conceptual—raise important questions regarding their political acceptability, military effectiveness, industrial feasibility, and strategic credibility. Translating such ambitions into practical arrangements would require a significant advancement in European defence integration, accompanied by a more comprehensive sharing of responsibilities, resources, and strategic decision-making (Fink 2026).

At the same time, substantial obstacles continue to constrain any fundamental restructuring of Europe's deterrence architecture. The development of new strategic capabilities would require considerable financial resources, extended implementation timelines, and significant political commitment. Furthermore, the complexity of achieving consensus among European states with differing strategic cultures, threat perceptions, and defence priorities presents an additional challenge. Public sensitivity regarding militarisation and defence spending further complicates efforts to pursue major changes in deterrence policy (Sauer 2025).

These constraints are reflected in the diversity of public attitudes across Europe. Research conducted by the British public opinion and market research organisation YouGov (YouGov 2025) indicates that European societies remain divided on defence spending, military modernisation, strategic autonomy, and the future role of alliances. While broad support exists across much of Europe for continued membership in NATO and recognition of Russia as a significant security challenge, important differences remain between regions. In general, states located in Northern and Eastern Europe tend to demonstrate stronger support for increased defence expenditure, enhanced military preparedness, and deeper security cooperation, whereas public opinion in parts of Western and Southern Europe often displays greater concern regarding the financial costs of rearmament, the risks associated with military escalation, and the balance between defence priorities and social spending.

As a result, public attitudes toward deterrence are shaped by competing imperatives. On one hand, the perceived threat posed by Russia has increased support for stronger defence capabilities, greater military readiness, and closer international cooperation. On the other hand, concerns regarding militarisation, budgetary pressures, and strategic escalation continue to influence political debates across several European countries. Consequently, increased defence spending and military modernisation are not universally perceived as automatic contributors to security; their acceptance depends heavily on national threat perceptions, confidence in collective defence arrangements, trust in political institutions, and preferences regarding the balance between European integration and national sovereignty in defence matters.

Beyond these political considerations, the debate surrounding deterrence also requires engagement with several fundamental conceptual issues. Over the past two decades, deterrence has evolved from a framework largely centred on nuclear weapons toward a more comprehensive and multidimensional concept. Contemporary deterrence encompasses military, political, economic, technological, informational, and societal dimensions. Within this broader understanding, credibility—the cornerstone of any deterrence posture—is no longer determined solely by the capability to conduct nuclear retaliation. Instead, it increasingly depends on political cohesion, strategic consistency, military readiness, industrial resilience, and the perceived ability to sustain collective action during periods of prolonged competition or crisis. Whereas deterrence during the Cold War was primarily based on the threat of nuclear escalation, subsequent technological developments and operational experience have underscored the importance of integrating conventional and nuclear capabilities into a coherent deterrence framework. The emergence of precision-guided munitions, long-range strike systems, integrated air and missile defence, cyber capabilities, space-based assets, and advanced ISR systems has expanded the range of instruments available for deterrence and coercion. Contemporary deterrence therefore rests upon a combination of conventional and nuclear capabilities, supported by resilient political institutions, defence-industrial capacity, and societal preparedness. Consequently, any discussion concerning the future of European deterrence must begin with the conventional dimension. Credible conventional forces, capable of denying aggression and imposing unacceptable costs on a potential adversary, constitute the foundation upon which broader deterrence architectures—including nuclear deterrence—are built.

In the contemporary security environment, effective deterrence is increasingly understood as a multi-domain and multilayered enterprise that integrates conventional and nuclear capabilities, resilience and readiness, national and collective defence, and transatlantic solidarity with growing European responsibility (Fink 2026, Sauer 2025).

5.6.4 Future of Europe's Nuclear Security Architecture

Since the emergence of nuclear weapons, the concept of extended deterrence has constituted a central pillar of Western security policy and strategic stability. The primary objective of extended deterrence has been to deter aggression against allies by extending the protection of a nuclear-armed state to non-nuclear partners, thereby reducing both the likelihood of major war and the incentives for allied states to develop independent nuclear capabilities. Throughout the Cold War and into the contemporary security environment, the United States extended nuclear deterrence commitment has remained a cornerstone of Euro-Atlantic security.

Within the NATO framework, extended deterrence is intrinsically linked to the principle of collective defence enshrined in Article 5 of the North Atlantic Treaty. In practical terms, it reflects the commitment that an attack against an Ally—whether through strategic attack or overwhelming conventional aggression—would engage the full spectrum of Allied capabilities, including the United States' strategic forces. The credibility of this commitment has long been a key factor in deterring potential adversaries while supporting the objectives of nuclear non-proliferation and Alliance cohesion.

However, evolving geopolitical conditions have generated renewed debate regarding the future effectiveness of extended deterrence. Several NATO members, including France and the United Kingdom, have argued that the contemporary security environment requires a reassessment of traditional deterrence concepts and may necessitate the adaptation, modernisation, or expansion of national and collective deterrence capabilities (Kacprzyk 2025).

This strategic reassessment is driven primarily by two interconnected developments that have significantly increased uncertainty within the European security environment. First, the Russia–Ukraine War and repeated Russian references to nuclear capabilities have returned nuclear deterrence to the forefront of European strategic thinking. Second, concerns about the long-term sustainability of the United States' security commitments, particularly amid potential shifts in American strategic priorities, have intensified discussions about Europe's ability to assume greater responsibility for its own security (Spatafora 2025). Broader geopolitical developments further reinforce these concerns. The emergence of a more contested international security environment, characterised by strategic competition among major powers, has highlighted the risks of excessive dependence on external security guarantees. In particular, the growing strategic alignment between Russia and China is frequently viewed as a challenge to the existing international order and to the effectiveness of Western deterrence mechanisms.

Through the combination of military modernisation, economic influence, technological competition, and strategic coordination, these actors seek to challenge the cohesion and credibility of Western security institutions, including NATO's deterrence posture. Against this backdrop, Europe faces a strategic dilemma involving two longstanding pillars of its security architecture: continued reliance on extended deterrence provided by the United States and adherence to the principles of nuclear non-proliferation. The debate increasingly centres on whether Europe should strengthen its own contribution to nuclear deterrence while preserving the integrity of the transatlantic security framework.

The development of an independent European nuclear deterrent, however, faces substantial structural, political, and institutional obstacles. Nuclear weapons remain under the exclusive sovereign control of nation-states. In the United States, ultimate authority over the employment of nuclear weapons resides with the President, while France maintains complete national control over its nuclear forces and does not integrate its deterrent into NATO's nuclear decision-making structures. Any future European deterrence arrangement would therefore need to reconcile national sovereignty with collective consultation and political legitimacy. A partial model for such consultation already exists within NATO through the Nuclear Planning Group, which provides a forum for Allied consultation on nuclear policy and deterrence issues. However, France does not participate in the Group, reflecting its longstanding commitment to maintaining the independence of its national deterrent.

Additional challenges include the absence of political consensus among European states, differing national threat perceptions, and the lack of a unified political authority capable of making rapid strategic decisions during a crisis. Furthermore, the establishment and maintenance of a credible nuclear deterrent would require substantial and sustained financial commitments, raising difficult questions regarding burden-sharing and political accountability. Consequently, while debates concerning European nuclear autonomy have gained prominence, the creation of a genuinely European nuclear deterrence architecture remains a highly complex undertaking. Current discussions, therefore, focus less on replacing the United States' extended deterrence commitment and more on strengthening Europe's contribution to the Alliance's broader deterrence and defence posture. At the same time, debates concerning the credibility of the U.S. nuclear guarantee continue to underscore the enduring importance of transatlantic cohesion while highlighting the practical, political, and strategic challenges associated with developing an autonomous European nuclear deterrent that would be both militarily credible and internationally recognised (Kacprzyk 2025, Spatafora 2025). The analysis above indicates that the future of nuclear deterrence in Europe is being shaped by a complex interplay of strategic, political, military, and institutional factors.

The Russia–Ukraine War has intensified discussions on the credibility of extended deterrence, the scope of European strategic responsibility, the challenge posed by Russian coercive nuclear signalling, and the long-term resilience of the Euro-Atlantic security architecture. The key issues arising from this debate are summarised in Table 9.

Table 9: Key Issues Shaping the Future of European Nuclear Deterrence and Security Architecture (Author)

Issue	Description	Strategic Implications
European Strategic Autonomy vs. NATO Dependence	Growing debate over the balance between continued reliance on U.S. extended deterrence and Europe's assumption of greater responsibility for its own security and defence.	Greater European responsibility is likely to strengthen burden-sharing, but deterrence credibility will remain closely linked to NATO cohesion and U.S. strategic commitments.
Role of France in European Nuclear Security	France remains the EU's only nuclear-weapon state with a fully autonomous deterrent and is increasingly viewed as a key contributor to the European pillar of deterrence.	May enhance the European contribution to deterrence while preserving the transatlantic framework and Alliance cohesion.
Potential European Nuclear Umbrella	France is the only nuclear-weapon state within the EU and possesses a fully autonomous nuclear deterrent.	Offers opportunities to strengthen European strategic responsibility but faces significant political, legal, and institutional constraints.
Russian Nuclear Coercion and Strategic Ambiguity	Russia increasingly combines nuclear signalling, strategic ambiguity, information operations, and cross-domain coercion to influence adversary decision-making and deter Western actions.	Requires NATO and European states to maintain credible deterrence, clear signalling, and robust escalation-management mechanisms.
Escalation Management	The risk of horizontal and vertical escalation remains a central feature of NATO–Russia strategic competition, particularly in a nuclear context.	Effective deterrence depends on maintaining strategic stability while preventing miscalculation or uncontrolled escalation.
Nuclear Non-Proliferation Concerns	Efforts to strengthen European deterrence must remain compatible with existing non-proliferation obligations and the broader international arms-control framework.	Necessitates balancing enhanced deterrence capabilities with long-term support for the Nuclear Non-Proliferation Treaty regime.
Lack of European Political Consensus	European states continue to differ in threat perceptions, strategic cultures, defence priorities, and views regarding deterrence and strategic autonomy.	Limits the prospects for rapid development of common European deterrence arrangements and decision-making structures.
Decision-Making Authority	Nuclear deterrence remains subject to sovereign national control, particularly in France and the United Kingdom, creating challenges for collective European arrangements.	Any future European framework will require effective consultation mechanisms while preserving national decision-making authority.
Nuclear Deterrence Capability Sharing	In France and the UK, nuclear capabilities remain under national control.	Creates challenges for any future collective European nuclear deterrence arrangement.
Integration of Conventional and Nuclear Deterrence	Contemporary deterrence is based on the integration of conventional forces, nuclear capabilities, missile defence, cyber capabilities, ISR, and societal resilience.	Reinforces the need for a multidomain and multilayered deterrence posture capable of addressing both military and non-military threats.
Protection of NATO's Eastern Flank	Frontline Allies perceive Russia as the principal security challenge and emphasise the need for credible forward defence and deterrence.	Continues to drive force posture adaptation, regional defence planning, and readiness initiatives across NATO.
Public Support and Political Legitimacy	Public attitudes toward deterrence, defence spending, and military modernisation vary considerably across Europe.	Sustained political legitimacy and societal support remain essential for long-term deterrence policies and defence investments.
Transatlantic Cohesion	The credibility of European security continues to depend on close cooperation between European Allies and North America.	Any enhancement of European deterrence should complement rather than weaken NATO's collective deterrence and defence posture.
Strategic Stability in Europe	The Russia–Ukraine War has reinforced deterrence as the primary mechanism for maintaining European security and managing long-term strategic competition.	Strategic stability will increasingly depend on resilience, credible deterrence, and the ability to sustain competition without uncontrolled escalation.

5.6.5 Opportunities for a European Nuclear Deterrence Architecture

A significant development in the evolution of European deterrence was the adoption of the Northwood Declaration in July 2025, through which the United Kingdom and France agreed to deepen bilateral cooperation in the nuclear domain. The declaration provides for enhanced coordination of deterrence policies, strategic consultations, and capability planning while preserving full national sovereignty over nuclear decision-making. For the first time, however, it introduces the prospect of a more closely aligned deterrence posture between Europe's two nuclear-armed powers.

Under the agreement, Paris and London committed to coordinating their strategic assessments and deterrence policies in response to threats deemed to pose an "extreme" risk to European security. Although the declaration does not establish a common nuclear command structure or specify operational employment mechanisms, it envisages closer consultation and planning to ensure that British and French nuclear capabilities can contribute in a complementary manner to the credibility of collective deterrence. This represents an important step toward enhancing the coherence of the European contribution to NATO's overall deterrence and defence posture.

The Northwood Declaration, therefore, serves two interconnected purposes: strengthening the credibility of collective deterrence within the Euro-Atlantic security framework and exploring a realistic model of intra-European nuclear cooperation based on shared strategic responsibility while maintaining sovereign national control over nuclear forces (Fraioli 2025).

France occupies a particularly important position in this debate. It remains the only member state of the EU possessing a fully autonomous nuclear deterrent, capable of sustaining the entire nuclear enterprise—from warhead design and production to delivery systems, command and control, and operational employment—without external dependence. The United Kingdom likewise maintains an independent nuclear deterrent under national political control, although elements of its sea-based deterrent benefit from long-standing technical cooperation with the United States.

As a result, France is uniquely positioned to influence the future development of European deterrence. This role has been repeatedly acknowledged by President Macron, who has consistently advocated a broader strategic dialogue on the contribution of French nuclear forces to European security (Rose 2025). Such proposals do not represent an entirely new concept. The potential European dimension of French nuclear deterrence was already discussed during the 1990s, when policymakers and strategists considered whether the political effects of the French Force de Frappe could extend beyond the defence of strictly national interests.

Today, the prospect of extending the deterrent value of French nuclear capabilities to support broader European security objectives has re-emerged in the wider debate on European strategic responsibility. While such an approach could strengthen the European pillar of deterrence and complement NATO's existing nuclear arrangements, it also raises complex political and strategic questions concerning decision-making authority, burden-sharing, strategic autonomy, and the future relationship between European defence initiatives and transatlantic solidarity. A more prominent French role in European deterrence could therefore become a defining element in shaping the balance between greater European strategic responsibility and the continued centrality of NATO's collective deterrence framework (Zadra 2025).

5.6.6 Towards a More Europeanized Deterrence Framework

At the same time, deeper nuclear integration within Europe would need to be carefully balanced against the principles of the international nuclear non-proliferation regime. Any expansion of European nuclear cooperation could raise questions regarding responsibility, consultation mechanisms, and political control over nuclear decision-making. Consequently, France would be required to reconcile its role as an independent nuclear power with its broader contribution to collective security within both the Euro-Atlantic framework and the established non-proliferation architecture.

France's autonomous nuclear deterrent nevertheless provides Paris with considerable strategic flexibility to reassess and adapt its security posture in response to the lessons of the Russia–Ukraine War and the evolving European security environment. Such adaptation does not imply any departure from the fundamental principles of nuclear deterrence. Rather, it points to the development of a broader spectrum of response options, including conventional and sub-strategic instruments capable of addressing crises that may not directly threaten France's vital national interests but nonetheless require a more robust response than diplomatic or economic measures alone can provide.

In this context, France has the potential to strengthen its capacity to respond credibly, proportionately, and across multiple domains to acts of coercion, hybrid activities, or military aggression directed against European allies and partners. Such capabilities would enhance both European collective security and the overall credibility of deterrence across the Euro-Atlantic area.

Developments undertaken by France and the United Kingdom during 2025 provide an important case study in how nationally controlled nuclear deterrents can contribute to broader collective security objectives. The Northwood Declaration[15] reflects this evolution. While preserving the sovereign decision-making authority of both governments, it establishes a framework for closer strategic coordination and consultation, thereby enhancing the coherence and credibility of the European contribution to deterrence. Although it does not create an autonomous European nuclear force, it represents a significant step toward greater European strategic responsibility, based on cooperation between states possessing nuclear capabilities and on the growing recognition that European security can no longer rely exclusively on external guarantees. The return of large-scale interstate war to Europe and the increasingly prominent role of nuclear signalling in Russian strategy have fundamentally altered the continent's security environment. As a result, Europe faces a critical strategic challenge: how to reconcile its long-standing reliance on the United States extended-deterrence commitment with the growing desire to strengthen its own contribution to deterrence and defence while remaining fully consistent with its non-proliferation obligations.

The analysis presented above illustrates how concerns regarding transatlantic cohesion, combined with the ambiguity and unpredictability of Russian strategic behaviour, have intensified debate regarding the long-term credibility and sustainability of extended deterrence. Within this context, France and the United Kingdom emerge as the principal actors capable of strengthening the European contribution to nuclear deterrence.

The Northwood Declaration of 2025 constitutes an important milestone in this process. By establishing unprecedented levels of strategic consultation and coordination between Europe's two nuclear powers, it enhances the credibility of deterrence while fully preserving national sovereignty over nuclear decision-making. Whether this initiative ultimately evolves into a broader European deterrence framework or remains primarily a bilateral arrangement remains uncertain. Important questions, therefore, remain unresolved. It is not yet clear to what extent such cooperation could contribute to the security of the Alliance's most exposed regions, including the Baltic States, Poland, Finland, and Romania, where perceptions of threat are particularly acute and where credible deterrence remains essential for maintaining regional stability.

[15] The Northwood Declaration is a landmark bilateral agreement signed on July 10, 2025, by British Prime Minister Keir Starmer and French President Emmanuel Macron at the UK's Northwood military headquarters. It establishes unprecedented coordination and planning regarding the independent nuclear deterrents of the UK and France to strengthen European security. The Northwood Declaration represents a major evolution in European defence by establishing a framework for the UK and France to coordinate their independent nuclear policies, capabilities, and strategic postures. This shift responds directly to rising geopolitical threats and anxieties over the long-term reliability of the U.S. security umbrella

Under current political and strategic conditions, the most realistic path forward is unlikely to involve creating a supranational European nuclear force. Rather, it lies in the gradual development of a structured framework for strategic consultation, coordination, and burden-sharing among European allies. Such an approach would be based on political trust, interoperability, shared strategic responsibility, and close integration with NATO's overall deterrence and defence posture. It is through this process that a stronger European contribution to deterrence may emerge, reinforcing both European security and the broader credibility of the Euro-Atlantic deterrence architecture.

The central issue for Europe is not whether nuclear deterrence remains necessary, but how to adapt deterrence to an increasingly contested security environment characterised by Russian nuclear coercion, uncertainty regarding long-term U.S. commitments, growing demands for European strategic responsibility, and the need to preserve both NATO cohesion and the nuclear non-proliferation regime.

CONCLUSIONS

The Russia–Ukraine War represents a defining case study in the evolution of contemporary high-intensity warfare, illustrating the transition from predominantly manoeuvre-centric operations towards a form of warfare characterised by attrition, persistent competition, and the integration of effects across multiple operational domains.

The analytical study met its primary objective by comprehensively assessing the evolving multi-domain operating environment of the Russia–Ukraine War from autumn 2023 to the end of 2025. It identifies the decisive characteristics of the operating environment, cross-domain interactions, and adaptation dynamics across all operational domains, providing analytically substantiated conclusions and implications relevant to the future development of Euro-Atlantic security.

Evolution of the Operational Character of the Russia–Ukraine War

During the period 2024–2025, the conflict was defined less by operational breakthroughs and more by the gradual degradation of military capabilities and war-sustaining systems, in which operational success increasingly depended on force generation, defence-industrial capacity, resilience, and the ability to sustain effects against the adversary.

A central conclusion of this study is the re-emergence of attrition as a dominant operational logic. Both belligerents increasingly focused on degrading adversary combat power, logistics, command-and-control systems, and defence-industrial capacity rather than achieving rapid territorial advances. The persistence of a heavily fortified frontline, combined with pervasive ISR coverage and the extensive employment of unmanned systems, significantly constrained operational manoeuvre. Consequently, military effectiveness became increasingly dependent on the cumulative generation of effects through fires, endurance, adaptation, and resilience, reinforcing the importance of time as a decisive strategic factor.

At the operational level, the study demonstrates that maintaining initiative—understood as the ability to impose operational tempo, shape conditions, and compel adversary reactions—has become a critical determinant of success. Since early 2024, the Russian Federation has progressively consolidated operational initiative through sustained offensive activity, superior force regeneration, and the integration of fires, unmanned systems, electronic warfare, and long-range strike capabilities. Ukraine, by contrast, increasingly adopted an economy-of-force approach focused on preserving combat power, disrupting Russian operations through deep strikes, and maintaining operational endurance through external support.

Another significant finding concerns the growing importance of operational and strategic depth. Long-range precision strikes against logistics networks, critical infrastructure, command-and-control nodes, and defence-industrial facilities have become integral components of operational design.

The conflict demonstrates that contemporary warfare spans the entire operating environment, in which strategic interdiction directly influences operational outcomes. This dynamic is further amplified by the integration of cyber operations, information activities, and electromagnetic warfare, all of which shape decision-making processes and influence strategic behaviour.

The conflict also confirms the emergence of an increasingly integrated and mature multi-domain operating environment, consistent with concepts outlined in the NATO Warfighting Capstone Concept and Strategic Foresight Analysis 2023. Operational effectiveness increasingly depends upon the synchronisation of effects across the land, maritime, air, cyber, space, and cognitive dimensions of warfare. Within this framework, the space domain has emerged as both a critical enabler and a contested domain, exerting a significant influence on the conduct of military operations.

Although the conflict has not involved large-scale kinetic engagements in space, it demonstrates the indispensable role of space-enabled capabilities in modern warfare. Space-based ISR, SATCOM, PNT services, and space-supported targeting networks provide essential support for C2 systems, operational awareness, targeting cycles, and force coordination. Ukraine's extensive reliance on commercial and Allied space capabilities has significantly enhanced operational resilience and combat effectiveness while compensating for limitations in sovereign space assets.

At the same time, the war highlights the vulnerability of space-enabled systems and the increasing convergence of the space and cyber domains. Cyberattacks against satellite networks, electronic attacks against GNSS signals, and information activities targeting space-supported systems demonstrate the growing importance of non-kinetic counterspace operations. Rather than relying primarily on destructive anti-satellite weapons, Russia has largely pursued actions below the threshold of major escalation through cyber interference, electronic warfare, signal disruption, and information operations designed to degrade adversary capabilities while limiting escalation risks.

The conflict also demonstrates the growing role of commercial actors within the operational environment. Commercial satellite imagery, communications services, and data analytics have become integral elements of military capability generation and operational effectiveness.

This development reflects a broader shift towards an increasingly interconnected defence ecosystem in which governmental, military, commercial, and civilian actors contribute to operational outcomes. Consequently, issues of resilience, governance, and the protection of commercially owned critical infrastructure assume increasing strategic importance.

The integration of space capabilities within broader military operations further reinforces the concept of system-of-systems warfare, a key theme of the NATO Warfighting Capstone Concept. Operational advantage is increasingly generated through the interaction of interconnected capabilities rather than through the isolated superiority of individual systems. As a result, disruptions in one domain can create cascading effects throughout the wider warfighting system, affecting command and control, situational awareness, targeting processes, force employment, and overall operational effectiveness.

Multi-Domain Convergence and Implications for New Security Architecture

From a strategic perspective, the conflict confirms that industrial capacity, technological adaptation, societal resilience, and the ability to sustain military operations over time have become decisive factors in high-intensity attritional warfare. The capacity to generate and replenish both advanced and low-cost capabilities—including unmanned systems and precision-strike assets—has emerged as a key determinant of strategic endurance. Within this context, space capabilities contribute not only to operational effectiveness but also to strategic resilience by enabling persistent connectivity, intelligence sharing, and multinational coordination. For NATO, these developments reinforce the principles articulated in the NATO 2022 Strategic Concept, the DDA Concept, the Strategic Foresight Analysis 2023, and the NATO Warfighting Capstone Concept. Collectively, these documents emphasise the need for integrated deterrence and defence, cognitive superiority, cross-domain command, power projection, and integrated multi-domain defence. The conflict highlights several critical priorities for future force development:

- integration of multi-domain operations and cross-domain effects;
- resilience of logistics, sustainment systems, and military mobility;
- strengthening the EDITB;
- the ability to operate effectively in contested cyber, space, and electromagnetic environments;
- enhancement of command-and-control structures capable of supporting cross-domain command and decision superiority;
- development of societal resilience and civil preparedness as components of comprehensive deterrence and defence.

The accession of Finland and Sweden further strengthens NATO's theatre-wide deterrence and defence posture, enabling a more integrated operational framework extending from the High North through the Baltic region to the Black Sea. However, the conflict demonstrates that credible deterrence increasingly depends upon readiness, resilience, sustainability, and the ability to generate combat power over time, rather than solely on the forward deployment of forces.

For the EU and the Common Security and Defence Policy (CSDP), the implications are complementary. The conflict underscores the necessity of strengthening the European Defence Technological and Industrial Base (EDTIB), enhancing cyber resilience, protecting critical infrastructure, securing space-enabled services, and adopting comprehensive whole-of-government and whole-of-society approaches to security. While existing EU initiatives contribute significantly to these objectives, the scale and duration of the conflict highlight the need for deeper integration, interoperability, and sustained investment.

At the strategic level, developments during 2024–2026 indicate that the conflict has evolved beyond a regional war into a broader condition of long-term NATO–Russia strategic competition characterised by persistent confrontation, deterrence, competition below the threshold of armed conflict, and carefully managed escalation. In this environment, strategic success is measured less by decisive victory and more by the ability to preserve resilience, maintain strategic freedom of action, and sustain long-term competitive advantage.

Ultimately, the study concludes that the contemporary phase of the Russia–Ukraine War is characterised by the convergence of attritional warfare and integrated multi-domain operations. Military effectiveness increasingly depends upon the ability to synchronise activities across all domains while sustaining industrial capacity, logistical endurance, societal resilience, and cognitive advantage over prolonged periods. For NATO and the EU, the principal lesson is clear: future deterrence and defence require integrated, resilient, and sustainable warfighting systems capable of operating effectively within a contested, transparent, and persistently competitive multi-domain operating environment.

ACRONYMS

AI	Artificial Intelligence
AEW&C	Airborne Early Warning and Control
ARF	Allied Reaction Force
ASAT	Anti-Satellite
ATACMS	Army Tactical Missile System
A2/AD	Anti-Access/Area Denial
CEMA	Cyber-Electromagnetic Activities
CEPA	Center for European Policy Analysis
CSDP	Common Security and Defence Policy
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
DDA	Deterrence and Defence of the Euro-Atlantic Area
DEAD	Destruction of Enemy Air Defences
DDoS	Distributed Denial-of-Service
EDTIB	European Defence Technological and Industrial Base
EEAS	European External Action Service
eFP	Enhanced Forward Presence
EMSO	Electro-Magnetic Spectrum Operations
EU	European Union
EW	Electronic Warfare
FPV	First-Person View
GDP	Gross Domestic Product
GLONASS	Global Navigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HIMARS	High Mobility Artillery Rocket Systems
IADS	Air Defence System
IAMD	Integrated Air and Missile Defence Systems
ISR	Intelligence, Surveillance and Reconnaissance
ISW	Institute for the Study of War
JFACC	Joint Force Air Component Commander
LEO	Low Earth Orbit
LLMs	Large Language Models
MAICAs	Military AI Cyber Agents

MDO	Multi-Domain Operations
MISO	Military Information Support Operations
NATO	North Atlantic Treaty Organization
NBIC	Nanotechnology, Biotechnology, Information Technology, and Cognitive Science
NFM	New NATO Force Model
NIS	Network and Information Security
NRF	NATO Response Force
OECD	Organisation for Economic Co-operation and Development
OSINT	Open-Source Intelligence
PGMs	Precision-Guided Munitions
PNIs	Presidential Nuclear Initiatives
PNT	Positioning, Navigation and Timing
PR	Personnel Recovery
RPO	Rendezvous and Proximity Operations
RAP	Readiness Action Plan
PSYOPS	Psychological Operations
SACEUR	Supreme Allied Commander Europe
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SEAD	Suppression of Enemy Air Defences
SHAPE/ACO	Supreme Headquarters Allied Powers Europe/Allied Command Operations
SIPRI	Stockholm International Peace Research Institute
SNF	Standing Naval Forces
tFP	Tailored Forward Presence
TTPs	Tactics, Techniques, and Procedures
UAS	Unmanned/ Uncrewed Aerial Systems
UAV	Unmanned Aerial Vehicle
USVs	Uncrewed Surface Vessels

REFERENCES

ACT (ed.). “NATO Warfighting Capstone Concept”. Allied Command Transformation. Public Affairs Office. Norfolk (VA): USA. 2021. https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf [cit. 2026-06-17]

ACT (ed.). “Strategic Foresight Analysis 2023”. Allied Command Transformation. Public Affairs Office. Norfolk (VA): USA. 2023. https://www.act.nato.int/wp-content/uploads/2024/05/SFA2023_rev2.pdf [cit. 2026-06-17]

Adamsky, Dmytri. “Nuclear Incoherence: Deterrence Theory and Non-Strategic Nuclear Weapons in Russia”. *Journal of Strategic Studies*, 37(1), 91–134. 2024. https://doi.org/10.1080/01402390.2013.798583 [cit. 2026-06-17]

Allen, Patrick and Dennis Gilbert. “The Information Sphere Domain Increasing Understanding and Cooperation”. NATO Cooperative Cyber Defence Centre of Excellence (NCCDCOE). Tallinn: Estonia. 2018. https://www.ccdcoe.org/uploads/2018/10/09_GILBERT-InfoSphere.pdf [cit. 2026-06-17]

Avdaliani, Emil. “Russia’s New Black Sea Base Angers Georgia”. Center for European Policy Analysis (CEPA). Washington (D.C.): USA. 2023. https://cepa.org/article/russias-new-black-sea-base-angers-georgia/

Baumann, Ingo. “GLONASS and PNT in Russia”. Inside GNSS Media & Research LLC. New Jersey: USA. 2016. https://insidegnss.com/glonass-and-pnt-in-russia/ [cit. 2026-06-17]

Biddle, Stephen. “Military Power: Explaining Victory and Defeat in Modern Battle”. Princeton University Press. ISBN: 978-0691128023. 2006. 28–51.

Bienvenue, Emily et al.” Private Tech Companies, the State, and the New Character of War. Carnegie Endowment for International Peace”. Washington (D.C.): USA. 2025. https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies [cit. 2026-06-17]

Bingen, Kari A. “Extending the Battlespace to Space. War and the Modern Battlefield: Insights from Ukraine and the Middle East”. Center for Strategic and International Studies (CSIS). Washington (D.C.): USA. 2025. https://www.csis.org/analysis/chapter-8-extending-battlespace-space [cit. 2026-06-17]

Black, James et al. “Enhancing deterrence and defence on NATO’s northern flank - Allied perspectives on strategic options for Norway”. RAND Corporation. Santa Monica (CA): USA. 2020.https://www.rand.org/content/dam/rand/pubs/research_reports/RR4300/RR4381/RAND_RR4381.pdf [cit. 2026-06-17]

Bollfrass, Alexander et al. “Space Capabilities to Support Military Operations in the European Theatre”. International Institute for Strategic Studie (IISS). London: UK. 2025. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/01/space-capabilities-to-support-military-operation/pub25-004-space-capabilities-military-ops-in-europe.pdf [cit. 2026-06-17]

Bondar, Kateryna. “How Ukraine Rebuilt Its Military Acquisition System Around Commercial Technology”. Center for Strategic and International Studies (CSIS). Washington (DC): USA. 2025. https://www.csis.org/analysis/how-ukraine-rebuilt-its-military-acquisition-system-around-commercial-technology [cit. 2026-06-17]

Brantly, Aaron. “Battling the Bear: Ukraine’s Approach to National Cyber and Information Security”. State of the Art of Cyber Security and Cyberconflict Research Conference, 27-29 September 2018. Zürich: Switzerland. 2018. https://vtechworks.lib.vt.edu/server/api/core/bitstreams/1e02aac1-e0cc-4aae-acfa-60bdec6f053f/content [cit. 2026-06-17]

Bryan, Frederick et al. “Consequences of the Russia-Ukraine War and the Changing Face of Conflict”. Research Brief RB-A3141-1. RAND Corporation. Santa Monica (CA): USA. 2025. https://www.rand.org/pubs/research_briefs/RBA3141-1.html [cit. 2026-06-17]

Châtelet Valentin and Amaury Lesplingart. “Russia-linked Pravda network cited on Wikipedia, LLMs, and X”. Digital Forensic Research Lab (DFRLab). Washington (DC): USA. 2025. https://dfrlab.org/2025/03/12/pravda-network-wikipedia-llm-x/ [cit. 2026-06-17]

CheckFirst (ed.). “Operation Overload: An AI fuelled escalation of the Kremlin-linked propaganda effort”. CheckFirst Helsinki: Finland. 2025. https://checkfirst.network/operation-overload-an-ai-fuelled-escalation-of-the-kremlin-linked-propaganda-effort/ [cit. 2026-06-17]

Chevassus, Ludovic. “L’attrition comme stratégie militaire”. *Les Clionautes. Réflexions géopolitiques*. Paris: France. 2025. https://www.clionautes.org/lattrition-comme-strategie-militaire.html [cit. 2026-06-17]

Clausewitz, Carl von. “On War”. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University, USA. Press, 1989.

Cranny-Evans, Sam. “Mapping the expansion of Russia’s defence industry”. ESD. Bonn: Germany. 2025. https://euro-sd.com/2025/09/articles/exclusive/46685/mappingthe-expansion-of-russias-defence-industry/ [cit. 2026-06-17]

Cooper, Julian. “Preparing for a fourth year of war: military spending in Russia's budget for 2025”. Stockholm International Peace Research Institute (SIPRI), No. 2025/04. Stockholm: Sweden. https://doi.org/10.55163/CBXJ2246 [cit. 2026-06-17]

Deptula, David A. “Air Superiority and Russia’s War on Ukraine”. *Air and Space Forces Magazine* July/August 2024. Arlington (VA): USA. 2024. https://www.airandspaceforces.com/article/air-superiority-and-russias-war-on-ukraine/ [cit. 2026-06-17]

Diaz de Leon Jose. “Understanding Multi-Domain Operations in NATO”. In: *The Three Swords Magazine n° 37*. Joint Warfare Centre Public Affairs Office. Stavanger, Norway. 2021. https://www.scribd.com/document/771974326/NATO-2021-Multi-Domain-Operation-issue37-21 [cit. 2026-06-17]

Dickey, Robin, and Michael P. Gleason. “Space and War in Ukraine: Beyond the Satellites.” *Æther: A Journal of Strategic Airpower & Spacepower* 3, no. 1. 2024. p 20–35. https://www.jstor.org/stable/48766059 [cit. 2026-06-17]

Dugoin-Clément,Christine. “Géopolitique de l'ingérence russe: La stratégie du chaos”. Presses Universitaires de France. Paris: France. 2025. ISBN 2130881475

Edwards, Charlie. “The Paradox of Russian escalation and NATO’s response”. IISS (International Institute for Strategic Studies). London: UK. 2025. https://www.iiss.org/online-analysis/online-analysis/2025/09/the-paradox-of-russian-escalation-and-natos-response/ [cit. 2026-06-17]

EEAS (ed.). White Paper for European Defence – Readiness 2030. The Diplomatic Service of the European Union, 2025. https://www.eeas.europa.eu/eeas/white-paper-for-european-defence-readiness-2030_en [cit. 2026-06-17]

Eken, Mattias, Kiran Suman-Chauhan, Beatrice Aubert, Paul van Hooft. “Understanding Russian strategic culture and the low-yield nuclear threat”. Research Report. RAND Europe. Santa Monica (CA). USA. 2025. https://www.rand.org/pubs/research_reports/RRA3859-1.html [cit. 2026-06-17]

Eli, Corin. “Presidential Nuclear Initiatives: An Alternative Paradigm for Arms Control”. Report Feb 29, 2004. Nuclear Threat Initiative. Washington (D.C.): USA. 2004. https://www.nti.org/analysis/articles/presidential-nuclear-initiatives/ [cit. 2026-06-17]

Engelbrekt Bakardjieva, Antonina et al. “The Borders of the European Union in a Conflictual World: Interdisciplinary European Studies”. Palgrave MacMillan. London: UK. 2024. ISBN 3031542029.

EU (ed.). “Resolution on Russia’s disinformation and historical falsification to justify its war of aggression against Ukraine”. 2024/2988(RSP). European Parliament. 23 January 2025 – Strasbourg: France. https://www.europarl.europa.eu/doceo/document/TA-10-2025-0006_EN.html [cit. 2026-06-17]

European Commission (ed.). “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”. Official Journal of the European Union L 194/1. Brussels: Belgium. 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148 [cit. 2026-06-17]

European Commission (ed.). “ReArm Europe Plan/Readiness 2030”. European Commission. Brussels: Belgium. 2025. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769566/EPRS_BRI(2025)769566_EN.pdf [cit. 2026-06-17]

Fink, Anya L. “U.S. Extended Deterrence and Regional Nuclear Capabilities” (CRS Report for Congress). Report IF12735 Congressional Research Service. 2026. https://www.legistorm.com/reports/view/crs/631557/U_S_Extended_Deterrence_and_Regional_Nuclear_Capabilities.html [cit. 2026-06-17]

Fraioli, Paul (ed.). “The Northwood Declaration: UK–France nuclear cooperation and a new European strategic backstop”. Strategic Comments. The International Institute for Strategic Studies (IISS). London: UK. ISSN: 1356-7888. 2025. https://www.tandfonline.com/doi/pdf/10.1080/13567888.2025.2555142 [cit. 2026-06-17]

Gady, Franz-Stefan and Michael Kofman. “Ukraine’s Strategy of Attrition”. *Survival, 65(2), 2023*, International Institute for Strategic Studies (IISS). London: UK. 2023. pp. 7–22. https://www.tandfonline.com/doi/full/10.1080/00396338.2023.2193092?scroll=top&needAccess=true#abstract [cit. 2026-06-17]

Galeotti, Mark. “I’m Sorry for Creating the ‘Gerasimov Doctrine”. *Foreign Policy Analytics*. Washington (DC): USA. 2018. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ [cit. 2026-06-17]

Greminger, Thomas and Tobias Vestner (ed.) “The Russia-Ukraine War’s Implications for Global Security: A First Multi-issue Analysis”. Geneva Centre for Security Policy. Geneva: Switzerland. 2022. https://www.gcsp.ch/sites/default/files/2024-12/gcsp-analysis-russia-ukraine-war-implications.pdf [cit. 2026-06-17]

Gris, Michelle et al. “Russia’s Military After Ukraine: Potential Pathways for the Postwar Reconstitution of the Russian Armed Forces”. Rand Corp. 2025. ISBN 978-1977414151

Hanzhang, Tao. Sun Tzu: “The Art of War”. Ware: Wordsworth, 1993. ISBN 1-85326-305-2.

Idarand, Tõnis. “For as Long as It Works: Russia’s Nuclear Signalling During Its War in Ukraine”. International Centre for Defence and Security (ICDS). Tallinn: Estonia. 2025. https://icds.ee/en/for-as-long-as-it-works-russias-nuclear-signalling-during-its-war-in-ukraine/ [cit. 2026-06-17]

Institute for the Study of War. “Assessed Control of Terrain in the Russo-Ukrainian War, November 30, 2025“ ISW 2025a. https://understandingwar.org/map/assessed-control-of-terrain-in-the-russo-ukrainian-war-november-30-2025-at-130-pm-et/ [cit. 2026-06-17]

Institute for the Study of War. “Interactive Map: Russia's Invasion of Ukraine. Assessed Control of Terrain in Ukraine as of December 2024”. ISW 2026a. https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375 [cit. 2026-06-17]

Institute for the Study of War. “Russian Offensive Campaign Assessment, February 17, 2024” Assessed Control of Terrain Around Donetsk as of February 17, 2024. ISW. 2024 https://understandingwar.org/map/assessed-control-of-terrain-around-donetsk-as-of-february-17-2024-300-pm-et/ [cit. 2026-06-17]

Institute for the Study of War. “Russian Offensive Campaign Assessment, July 2, 2025”. Assessed Russian Advances in Kursk Oblast March 3, 2025 to March 11, 2025. ISW 2025b https://understandingwar.org/map/assessed-russian-advances-in-kursk-oblast-march-3-2025-to-march-11-2025/ [cit. 2026-06-17]

Institute for the Study of War. “Ukraine’s Strike Campaign Against Russian Counter-Air and Counter-Drone Defenses“. ISW 2026b. https://understandingwar.org/map/ukraines-strike-campaign-against-russian-counter-air-and-counter-drone-defenses-confirmed-and-reported-strikes-as-of-may-24-2026/ [cit. 2026-06-17]

Jones, Andy and Dmitry Melnikov. “Masquerade Attacks and the process of their detection”. Conference: 3rd European Conference on Information Warfare and Security. Royal Holloway, University of London: UK. 2004. ISBN: 0-9547096-2-4.

Jordash, Wayne et al. “Manufacturing Impunity: Russian Information Operations in Ukraine — Russia’s Use of Information Alibis and How They Materially Contribute to the Planning, Execution and Cover-up of International Crimes”. Global Rights Compliance. The Hague: the Netherlands. 2025. https://globalrightscompliance.org/wp-content/uploads/2025/05/Manufacturing-Impunity.pdf [cit. 2026-06-17]

Kacprzyk, Artur. “France, UK to Coordinate on Nuclear Deterrence”. Polish Institute of International Affairs (PISM). Warsaw: Poland. 2025. https://www.pism.pl/publications/france-uk-to-coordinate-on-nuclear-deterrence [cit. 2026-06-17]

Kaushal, Sidharth and Darya Dolzikova. “The Evolution of Russian Nuclear Doctrine. Occasional Papers”. The Royal United Services Institute for Defence and Security Studies (RUSI). London: UK. 2025. https://www.rusi.org/explore-our-research/publications/occasional-papers/evolution-russian-nuclear-doctrine [cit. 2026-06-17]

Kilinc, Noah Ugur. “Integrated Autonomous Maritime Strategy: Naval Transformation and Geopolitical Competition in the Twenty- First Century”. Research Gate. 2026. DOI: 10.13140/RG.2.2.30542.93767 [cit. 2026-06-17]

Klein, Lisa-Martina. “Maritime strategy: NATO countries intend to invest in sea mines and aircraft carriers”. *Briefings*. Media GmbH. Berlin: Germany. 2025. https://table.media/en/security/news/maritime-strategy-nato-countries-intend-to-invest-in-sea-mines-and-aircraft-carriers [cit. 2026-06-17]

Kofman, Michael. “Russian Maritime ‘A2/AD’: Strengths and weaknesses”. *Russia Military Analysis*. Blog on the Russia Military. 2020a. https://russianmilitaryanalysis.wordpress.com/2020/01/29/russian-maritime-a2-ad-strengths-and-weaknesses/ [cit. 2026-06-17]

Kofman, Michael, Anya Fink, Jeffrey Edmonds. “Russian Strategy for Escalation Management: Evolution of Key Concepts”. DRM-2019-U-022455-1Rev. Center for Naval Analyses (CAN). Arlington (VA): USA. 2020b. https://www.cna.org/reports/2020/04/DRM-2019-U-022455-1Rev.pdf [cit. 2026-06-17]

Kolomychenko, Maria. “Russia’s Fight Against “Foreign Agents” and How to Prevent Its Spread”. German Council on Foreign Relations Analysis No: 3. Berlin: Germany. 2025. ISSN 1611-7034. https://dgap.org/en/research/publications/russias-fight-against-foreign-agents-and-how-prevent-its-spread [cit. 2026-06-17]

Kott, Alexander. “Autonomous Intelligent Cyber-Defense Agent: Introduction and Overview”. *Advances in Information Security*, vol 87/2023. Springer, Cham. In book: Autonomous Intelligent Cyber Defense Agent (AICA). Print ISBN 978-3-031-29268-2. https://www.researchgate.net/publication/371275745_Autonomous_Intelligent_Cyber-defense_Agent_Introduction_and_Overview [cit. 2026-06-17]

Laird, Robbin. “A Paradigm Shift in Maritime Operations: Autonomous Systems and Their Impact (Airpower and Maritime Force Modernization)”. Second Line of Defense. Arlington, VA: USA. 2025. ISBN 979-8990786769

Lough, John et al. “There’s no military mobilisation in Russia, yet people are being mobilised” New Eurasian Strategies Centre. London: UK. 2024. https://nestcentre.org/october-2024-theres-no-military-mobilisation-in-russia-yet-people-are-being-mobilised/ [cit. 2026-06-17]

Luzin, Pavel and Evgeny Roshchin. “Russia’s Strategy and Military Thinking: Evolving Discourse by 2025”. Comprehensive Reports. Center for European Policy Analysis (CEPA). Washington (DC): USA. 2025. https://cepa.org/comprehensive-reports/russias-strategy-and-military-thinking-evolving-discourse-by-2025/ [cit. 2026-06-17]

MacAlpine, Audrey. “Four Key Instruments of Russian Propaganda: Dismiss, Distort, Distract, Dismay”. United24.media. 2025. https://united24media.com/anti-fake/instruments-of-russian-propaganda-dismiss-distort-distract-dismay-4899 [cit. 2026-06-17]

Melkozerova, Veronika. “How Ukraine is revamping frontline fortifications to stem Russian advances”. *Politico Europe*. 2025. https://www.politico.eu/article/ukraine-russia-drone-fortifications-frontline-defense/ [cit. 2026-06-17]

Mearsheimer, John. “The Tragedy of Great Power Politics”. Taibei Shi: Mai tian chu ban, 2001. ISBN 9780393323962.

Microsoft (ed.). “Microsoft Digital Defense Report 2025”. *Microsoft Security*. 2025. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025 [cit. 2026-06-17]

Minarik, Tomas. “NATO Recognises Cyberspace as a ‘Domain of Operations’ at Warsaw Summit”. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Tallin: Estonia. 2016. https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/ [cit. 2026-06-17]

Mowthorpe, Matthew and Markos Trichas. “The successful development of Russia’s counterspace activities in LEO and GEO”. *The Space Review*. 2026. https://www.thespacereview.com/article/5138/1 [cit. 2026-06-17]

NATO (ed.) “Deterrence and Defence of the Euro-Atlantic Area”. NATO HQs Brussels: Belgium. 2025a. https://www.nato.int/en/what-we-do/deterrence-and-defence/deterrence-and-defence [cit. 2026-06-17]

NATO (ed.). “NATO’s annual nuclear exercise Steadfast Noon begins”. News 13 October 2025. 2025b. NATO HQs Brussels: Belgium. https://www.nato.int/en/news-and-events/articles/news/2025/10/13/natos-annual-nuclear-exercise-steadfast-noon-begins [cit. 2026-06-17]

NATO (ed.). “NATO’s overarching Space Policy”. NATO HQs. Press Office. Brussels: Belgium. 2019. Online: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2019/06/27/natos-overarching-space-policy [cit. 2026-06-17]

NATO (ed.). “NATO 2022 Strategic Concept”. NATO HQs. Press Office. Brussels: Belgium. 2022. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf [cit. 2026-06-17]

Nesselhuf, F. Jon. “Failure in Ukraine Will Not Change the Russian Aerospace Defense Force”. *Military Review (MR)* January-February 2025. Army University Press. Fort Leavenworth, Kansas: USA. 2025. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2025/Meeting-Expectations/ [cit. 2026-06-17]

Nocetti, Julien. ”Enhanced subversion?”. Concepts and actors in the Russian cyber strategy. Presses Universitaires de France. National cyber strategies: Case studies. (2024). Études françaises de renseignement et de cyber (No 2). Paris: France. 2024. https://shs.cairn.info/journal-etudes-francaises-de-renseignement-et-de-cyber-2024-1?lang=en [cit. 2026-06-17]

OCS (ed.). “NATO Chief Scientist Research Report on Cognitive Warfare”. NATO STO Office of the Chief Scientist. Brussels: Belgium. 2025. https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare-4.pdf [cit. 2026-06-17]

OECD (ed.) “OECD Economic Surveys: Ukraine 2025”. OECD Publishing. Paris: France. Online: https://doi.org/10.1787/940cee85-en [cit. 2026-06-17]

OECD (ed.). “The Space Economy in Figures: Responding to Global Challenges”. OECD Publishing. Paris: France. 2023. ISBN 978-92-64-43195-9 (HTML). https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/12/the-space-economy-in-figures_4c52ae39/fa5494aa-en.pdf [cit. 2026-06-17]

Ogden, Theodora et al. “The Role of the Space Domain in the Russia-Ukraine War”. Expert Analysis. Centre for Emerging Technology and security (CETS). London: UK. 2024. https://cetas.turing.ac.uk/publications/role-space-domain-russia-ukraine-war [cit. 2026-06-17]

Olejnik, Lukasz. “Russian cyber and information warfare and its impact on the EU and UK”. King's College London: UK. 2025. https://www.kcl.ac.uk/russian-cyber-and-information-warfare-and-its-impact-on-the-eu-and-uk [cit. 2026-06-17]

Petráš, Zdeněk et al. “Analysis of Operating Environment in Ukraine – Course of the Conflict since February 2022 to Fall 2023”. University of Defence, Brno: Czech Republic. 2024. ISBN 978-80-7582-483-7.

Place, Joseph. Ukraine Now Leads in Deep Strikes. Is There “Safe Rear” Left for Russia? War in Ukraine. United24 Media. 2026. https://united24media.com/war-in-ukraine/ukraine-now-leads-in-deep-strikes-is-there-safe-rear-left-for-russia-18525 [cit. 2026-06-17]

Pobjie, Erin et al. “Advancing European Military Capacity in Space”. Research Papers. International Institute for Strategic Studies (IISS). London: UK. 2026. https://www.iiss.org/research-paper/2026/03/advancing-european-military-capacity-in-space/ [cit. 2026-06-17]

Polishchuk, Olha, Nichita Gurcov. “Bombing into Submission: Russian Targeting of Civilians and Infrastructure in Ukraine”. Armed Conflict Location & Event Data Project. JSTOR. 2025. http://www.jstor.org/stable/resrep67742 [cit. 2026-06-17]

Popa, Aurel and Sorin Learschi. “Russia’s strategic naval collapse in the context of the war in Ukraine (2022-2025)”. Study Maritime Security Forum. Bucharest: Romania. 2025. https://www.forumulsecuritatiimaritime.ro/russias-strategic-naval-collapse-2022-2025-in-the-context-of-the-war-in-ukraine/ [cit. 2026-06-17]

Rose, Michel. “France’s Macron’s address to the French nation on ramping up defence spending.” Reuters World., 5 March 2025. https://www.reuters.com/world/europe/frances-macronaddress-nation-late-wednesday-2025-03-05/ [cit. 2026-06-17]

RSF (ed.). ”World Press Freedom Index 2025: economic fragility a leading threat to press freedom”. Reporters Without Borders. Paris: France. 2025. https://rsf.org/en/rsf-world-press-freedom-index-2025-economic-fragility-leading-threat-press-freedom [cit. 2026-06-17]

Sakwa, Richard. “Russia Against the Rest: The Post-Cold War Crisis of World Order”. Cambridge University Press: UK. 2017. ISBN 9781316675885.

Samson, Victoria and Kathleen Brett. “2026 Global Counterspace Capabilities Report”. Annual report. Secure World Foundation. Washington (D.C.): USA. 2026. https://www.swfound.org/publications-and-reports/2026-global-counterspace-capabilities-report [cit. 2026-06-17]

SHAPE/ACO (ed.). “Eastern Sentry to enhance NATO’s presence along its eastern flank”. SHAPE Newsroom. Mons: Belgium. 2025. https://shape.nato.int/news-releases/eastern-sentry-to-enhance-natos-presence-along-its-eastern-flank [cit. 2026-06-17]

Slusher, Matthew. “Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience”. Center for Strategic and International Studies (CSIS). Washington (DC): USA. 2025. https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience [cit. 2026-06-17]

Sauer, Tom. “Towards a Eurobomb: The Costs of Nuclear Sovereignty”. Toda Peace Institute. Tokyo: Japan. 2025. https://toda.org/global-outlooks/towards-a-eurobomb-the-costs-of-nuclear-sovereignty/ [cit. 2026-06-17]

Sorg, Alexander. “Force de l’Europe: How Realistic is a French Nuclear Umbrella?”. War on the Rocks. Washington (DC): USA. 2025. https://warontherocks.com/force-de-leurope-how-realistic-is-a-french-nuclear-umbrella/ [cit. 2026-06-17]

Sadeghi, McKenzie. “AI False Information Rate Nearly Doubles in One Year”. NewsGuard. New York, NY: USA. 2025. https://www.newsguardtech.com/wp-content/uploads/2025/09/August-2025-One-Year-Progress-Report-3.pdf [cit. 2026-06-17]

Spatafora, Giuseppe (ed.). “The Trump card: What could US abandonment of Europe look like?”. Briefs. European Union Institute for Security Studies (EUISS). Brussels: Belgium. 2025. https://www.iss.europa.eu/publications/briefs/trump-card-what-could-us-abandonment-europe-look [cit. 2026-06-17]

Spencer, John, Liam Collins. “Twelve Months of War in Ukraine Have Revealed Four Fundamental Lessons on Urban Warfare”. Modern War Institute. Arlington, VA: USA. 2023. https://mwi.westpoint.edu/twelve-months-of-war-in-ukraine-have-revealed-four-fundamentallessons- on-urban-warfare/ [cit. 2026-06-17]

Statista (ed.). “Number of military conscripts in Russia 2012-2025”. Statista research Department. New York: USA. 2026. https://www.statista.com/statistics/1334431/russia-number-of-conscripts/?srsltid=AfmBOoouWLiWO6tIE14aIe1wGAKZEQiY7Bo1IG-ebeUCgcta08Oc_NZx [cit. 2026-06-17]

Sutter, Thierry. “Air Surface Integration, the Basis for Air-Ground Combat”. Cahier - 17-06-2019. La Revue Défense Nationale. Paris: France. 2019. https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=123&cidcahier=1183 [cit. 2026-06-17]

Thomas, Timothy. “Russia's Reflexive Control Theory and the Military”. *The Journal of Slavic Military Studies*, *17*(2), 237–256. 2010. https://doi.org/10.1080/13518040490450529 [cit. 2026-06-17]

Tkachuk, Nataliya. “Ukraine as the Frontline of European Cyber Defence: Building Resilience in the Face of Russian Cyber Aggression”. Tallinn Paper No. 15. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Tallin: Estonia. 2025. https://www.ccdcoe.org/uploads/2025/07/Tkachuk_N_Tallinn_Paper_15_Ukraine-as-the-Frontline-of-European-Cyber-Defence.pdf [cit. 2026-06-17]

Trevithick, Joseph. “Anduril Introduces Barracuda-M That Aims To Disrupt The Cruise Missile Market”. The War Zone Publisher. Miami (FL): USA. 2024. https://www.twz.com/air/anduril-introduces-barracuda-m-that-aims-to-disrupt-the-cruise-missile-market [cit. 2026-06-17]

Trevithick, Joseph. “Cheap Cruise Missile Paired With Affordable Seeker From Ship-Killing Smart Bomb Eyed By USAF”. The War Zone Publisher. Miami (FL): USA. 2025. https://www.twz.com/air/cheap-cruise-missile-paired-with-affordable-seeker-from-ship-killing-smart-bomb-eyed-by-usaf [cit. 2026-06-17]

Trusch, Sven. “From concept to capability: Multi-Domain Operations”. *NITECH 14/2025.* NATO Communications and Information Agency (NCI Agency). 2025. https://systematic.com/us/industries/defense/news-knowledge/blog/from-concept-to-capability-multi-domain-operations/ [cit. 2026-06-17]

Vanaga, Nora, Toms Rostoks. “Deterring Russia in Europe Defence Strategies for Neighbouring States”. Routledge. London: UK. 2019. ISBN 9780367585433

Vershinin, Alex. “The Attritional Art of War: Lessons from the Russian War on Ukraine”. Commentary. RUSI. London: UK. 2024. https://www.rusi.org/explore-our-research/publications/commentary/attritional-art-war-lessons-russian-war-ukraine [cit. 2026-06-17]

Viasat (ed.). “KA-SAT Network cyber attack overview.” *Perspectives*. Viasat, Inc. Carlsbad (CA): USA. 2022. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/ [cit. 2026-06-17]

Viginum (ed.).” Analysis of the Russian information manipulation set Storm-1516”. General Secretariat for Defence and National Security. Paris: France. 2025. https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf [cit. 2026-06-17]

Viginum (ed.). “Matryoshka - A pro-Russian campaign targeting media and the fact-checking community”. General Secretariat for Defence and National Security. Paris: France. 2024. https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf [cit. 2026-06-17]

Voo, Julia and Virpratap Vikram Singh. “Russia’s information confrontation ecosystem”. Charting Cyberspace. Institute for Strategic Studies (IISS). Washington (D.C.): USA. 2025. https://www.iiss.org/charting-cyberspace/2025/06/russias-information-confrontation-ecosystem/ [cit. 2026-06-17]

Waltz, N. Kenneth. “Theory of International Politics”. McGraw-Hill. Columbus (OH): USA. ISBN 0075548526. 1979.

Weichert, Brandon J. “Russia’s Space War for Ukraine is Just Getting Started”. *The Dossier*. New Lines Institute for Strategy and Policy. Washington D.C.): USA. 2022. https://newlinesinstitute.org/wp-content/uploads/20220825-Russia-Space-War-Dossier-NLISAP.pdf [cit. 2026-06-17]

Wiswesser, Sean M. “Potemkin on the Dnieper: the Failure of Russian Airpower in the Ukraine war”. *Small Wars & Insurgencies*, *34*(7), p. 1205–1234. 2023. https://doi.org/10.1080/09592318.2023.2187201 [cit. 2026-06-17]

YouGov (ed.). “European Political Monthly: Europeans on Defence and NATO”. YouGov PLC. London: UK. 2025. https://yougov.com/en-gb/articles/53219-european-political-monthly-europeans-on-defence-and-nato [cit. 2026-06-17]

Zadra, Roberto. “Can France Provide European Allies with Nuclear Deterrence?”. IAI Commentaries. Istituto Affari Internazionali. Rome: Italy. ISSN 2532-6570. 2025. https://www.iai.it/sites/default/files/iaicom2513.pdf [cit. 2026-06-17]

INDEX

Author: Zdeněk Petráš

Graphic Design and Editing: Eva Abrahámová

Publisher: University of Defence Brno, Czech Republic

Printed by: University of Defence Press Brno, Czech Republic

Number of Pages: 166

Year of Publication: 2026

Edition: First Edition

The publication has not undergone professional language editing.

ISBN 978-80-7582-688-6

ISBN 978-80-7582-689-3 (online; pdf)