

The Future of Warfare: Operational Lessons from Ukraine's 2026 Counteroffensive – The new military strategy: "Logistics Lockdown"

Dr Darko Trifunovic

(Senior Research Fellow of RIEAS and Director of INIS)

**Copyright: @ 2026 Research Institute for European and American Studies (www.rieas.gr)
Publication date: 29 May 2026**

Note: The article reflects the opinion of the author and not necessarily the views of the Research Institute for European and American Studies

The Ukrainian "Logistics Lockdown" concept demonstrates the emergence of a new model of operational-depth warfare in which the primary objective is not the immediate destruction of frontline forces, but the systematic paralysis of the enemy's operational ecosystem, including logistics, command structures, communications, ammunition depots, fuel reserves, transportation networks, and reinforcement corridors. Modern armed conflict in Ukraine has given us a new picture that the character of armed conflict has radically changed. The operations conducted during May 2026 in the sectors of Zaporizhzhia, Donetsk, Sumy, and Kherson represent one of the most important demonstrations of the transformation of modern warfare since the beginning of the conflict in 2022. According to Ukrainian sources, approximately 590 km² of territory was liberated during these coordinated operations, significantly undermining Russia's planned major summer offensive in southern Ukraine.

Russian strategy was based on the concentration of massive military force in the Zaporizhzhia region. In this sector, Russia deployed the elite 58th Combined Arms Army, including the 42nd Guards Motor Rifle Division, VDV airborne units, the 810th Naval Infantry Brigade redeployed from Crimea, and the notorious Storm-Z penal battalions. Moscow relied on deeply entrenched trench systems, minefields, and multilayered defensive positions to stabilize the front and later launch further offensives against Ukrainian positions. However, the Ukrainian command drew

important lessons from the 2023 failed offensives. During those operations, large mechanized columns frequently advanced directly into minefields, where they were destroyed by concentrated artillery fire and drone strikes. The new doctrine introduced in 2026 completely abandoned the concept of mass frontal assaults and instead implemented a model of intelligent, decentralized, and technologically integrated warfare. The main axis of the operation unfolded in the area of Hulyaipole and Tokmak in Zaporizhzhia. Between May 20 and 23, 2026, the Ukrainian 118th and 65th Mechanized Brigades launched carefully prepared nighttime infiltration operations toward the village of Zaliznychne west of Hulyaipole.

Instead of employing large armored formations, Ukraine deployed massive swarms of FPV drones equipped with night-vision systems that systematically destroyed Russian logistical trucks transporting ammunition and fuel to the front lines. Once the Russian frontline lost logistical support, Ukrainian infantry carried out rapid penetrations into the northern parts of the settlement after precise artillery strikes had softened them. A particularly significant operation took place on the Malo Machka–Bohyra axis between May 17 and 20, 2026. This area represented one of the key geographical elevations protecting the Russian corridor toward the south and Tokmak.

During the operation, Ukrainian forces employed a combination of electronic warfare, drones, and precise Western-made artillery systems. Ukrainian electronic warfare systems paralyzed Russian radio communications and command networks, while hundreds of FPV drones had previously mapped Russian bunkers, trenches, and ammunition depots. This was followed by precision artillery fire guided by airborne laser designation. Only after Russian command and logistics had been thoroughly disrupted did small Ukrainian mechanized groups begin infiltrating through narrow passages between minefields and anti-tank obstacles known as "dragon's teeth."

Unlike earlier attempts, Ukrainian units now operated in small flexible groups that mutually covered each other's maneuvers. Russian elements of the 42nd Guards Motor Rifle Division, as well as parts of the 71st and 291st regiments, were forced to withdraw due to the collapse of coordination and communication. The liberation of Malo Machka and Bohyra opened access to one of the key northern routes toward Tokmak — the logistical center of Russian defenses on the southern front. This seriously endangered the land corridor to Crimea, which represented the most important logistical artery for Russian forces in southern Ukraine.

Simultaneously with operations in Zaporizhzhia, Ukraine conducted coordinated asymmetric operations in forested areas toward Sumy and Kharkiv. Air assault brigades used light maneuver and infiltration through forest corridors where Russian mechanized forces could not effectively operate. In the east, near Kostyantynivka and Pokrovsk in Donetsk, Ukraine, the 47th Mechanized Brigade and unmanned systems units carried out deep strikes against ammunition depots, railway lines, command posts, and fuel bases. One of the most significant strikes occurred on May 23, 2026, in Oleshky on the eastern bank of the Dnipro River in Kherson Oblast.

A Russian drone command center responsible for directing artillery fire against Ukrainian positions was located there. Ukrainian FPV drones conducted a precise strike during a shift change and refueling process, destroying the facility and eliminating several Russian drone operators. The attack had a major psychological effect, as even Russian propaganda channels were forced to acknowledge the scale of the loss. The essence of the Ukrainian operation was not the classical Soviet-style seizure of territory through mass armored assaults, but the systematic destruction of Russian operational capability. By targeting logistics, communications, and command centers, Russian forces were gradually brought into a state of paralysis.

The war in Ukraine confirms several fundamental transformations in modern warfare

First, logistics has become the central objective of war. Modern conflicts in Ukraine demonstrate that the enemy is no longer destroyed primarily through frontal clashes of massive armored formations, but through the systematic destruction of its ability to sustain combat operations. An army without fuel, ammunition, spare parts, medical support, and stable communications can no longer maintain even the strongest fortification systems. Deep trenches, concrete bunkers, minefields, and multilayered defenses become practically useless once units are deprived of artillery ammunition, food, fuel, and coordination with command structures. Ukrainian operations in 2026 were based precisely on this principle. Instead of directly destroying every Russian position, priority was given to systematically attacking logistical trucks,

ammunition depots, railway routes, fuel bases, and command centers. FPV drones were used as "hunter groups" that monitored supply routes for hours and destroyed vehicles attempting to deliver ammunition to frontline positions. Once logistical flows were disrupted, Russian units became isolated in their own trenches, unable to organize effective resistance. At the same time, electronic warfare further paralyzed command structures. The loss of radio links and digital communications created chaos among frontline units. Without coordination between artillery, reconnaissance, and infantry, even numerically superior forces became operationally blind. Modern logistics is therefore no longer merely about transporting ammunition and food, but also about preserving the army's information and communication systems.

Second, drones have become the dominant instrument of the battlefield. The war in Ukraine has shown that unmanned systems are no longer merely auxiliary reconnaissance tools, but the central element of modern warfare, integrating reconnaissance, targeting, psychological pressure, destruction of equipment, electronic warfare, and control of operational space. FPV drones, in particular, have had a revolutionary impact. These relatively inexpensive systems can precisely strike tanks, bunkers, artillery systems, logistical vehicles, or individual trenches. A drone worth only a few hundred dollars can destroy a multimillion-dollar tank or severely damage a complex air defense system. This has fundamentally altered the economic balance of warfare. Ukrainian operations during 2026 demonstrated a high degree of drone integration at all levels of combat. Before attacks, drones spent months mapping Russian trenches, minefields, bunkers, and ammunition depots. During operations, they simultaneously identified targets, disrupted logistics, directed artillery fire, transmitted battlefield data, and conducted kamikaze strikes. The war in Ukraine has also demonstrated that drones have practically eliminated the traditional ability to conceal large military formations. Any movement of columns, concentration of troops, or attempt to deliver reserves can now be detected almost instantly from the air. Modern armies have therefore lost the ability to conduct prolonged concealed maneuvering in open terrain.

Third, electronic warfare has become as important as artillery and airpower. Modern armies no longer depend solely on tanks, artillery, and manpower, but primarily on the stability of their communication and information systems. Whoever loses communications, satellite links, navigation systems, and digital space effectively loses the ability to command, coordinate, and organize resistance. Ukrainian operations in 2026 clearly demonstrated how electronic warfare can alter the course of battle. Before attacks, Ukrainian electronic warfare systems paralyzed Russian radio communications and disrupted coordination between command structures, artillery, reconnaissance, and logistics. In certain sectors, Russian units became completely isolated from command and unable to receive orders or information about the direction of attack. Electronic warfare today extends far beyond traditional radio jamming. Modern systems can disrupt GPS navigation, jam drones, intercept communications, manipulate signals, create false targets, and effectively blind enemy forces. The battlefield has thus become a digital environment where an invisible war for control of information and data flows takes place.

Fourth, massive armored formations are becoming increasingly vulnerable to small, inexpensive, and precise unmanned systems. The war in Ukraine has shown that the concept of large concentrations of tanks and armored vehicles — which for decades underpinned land power for major armies — is entering a profound crisis. Large armored columns that once symbolized operational breakthroughs and dominance are now ideal targets for drones, precision artillery, and electronic surveillance. Once concentrations of equipment are detected, they are rapidly subjected to coordinated FPV drone strikes, precision artillery fire, and attacks on logistical routes. The relationship between the cost of weapons and battlefield effect has changed dramatically. A relatively cheap FPV drone can destroy a multimillion-dollar armored vehicle. As a result, massive armored formations increasingly become logistical burdens requiring enormous amounts of fuel, ammunition, spare parts, and anti-drone protection. The war in Ukraine therefore demonstrates that tanks have not disappeared from the battlefield; they have, however, lost the dominant role they held throughout the twentieth century. Armored systems remain important for infantry support, protection, and firepower. Still, they can no longer

independently determine the outcome of battles without complete integration with drones, electronic warfare, and precision reconnaissance systems.

Fifth, the war in Ukraine demonstrates that information operations and psychological effects have become an integral component of every military success. Modern warfare is no longer fought exclusively on the frontline, but simultaneously in cyberspace, the media environment, social networks, information platforms, and the global digital sphere. The war in Ukraine has become the first truly globally digitalized conflict in which millions of people follow operations in real time through Telegram channels, drone footage, satellite imagery, and social media. A completely new battlefield of perception has emerged where victory depends not only on territorial control but also on control of the war narrative. Psychological effects now directly influence military operations. Constant drone attacks, publication of destroyed equipment footage, and continuous media emphasis on enemy losses create fear, exhaustion, and uncertainty among soldiers. The modern soldier is exposed not only to physical danger but also to continuous psychological pressure generated by digital surveillance and media exposure. Cyber operations have likewise become an integral component of military planning. Attacks against communication systems, energy infrastructure, state servers, satellite links, and digital networks can have consequences almost as severe as traditional air strikes. War therefore extends far beyond the frontline and penetrates the everyday life of entire societies. For countries such as Serbia, the lessons from Ukraine represent an extremely serious warning and perhaps the most important military-security lesson of the twenty-first century. Future wars will not be decided solely by the number of tanks, artillery systems, or troop strength, but by the ability to integrate drones, autonomous systems, electronic warfare, AI technologies, cyber capabilities, precision artillery, satellite reconnaissance, intelligence operations, and highly mobile small units operating within networked systems.

The war in Ukraine has shown that modern armed forces must function as unified digital-information organisms in which reconnaissance, communications, data analysis, precision firepower, and command structures are connected almost in real time. Traditional models of slow command processes, rigid hierarchies, and mass concentration of equipment are becoming

increasingly vulnerable to fast, flexible, and technologically adaptive opponents. Intelligence services and intelligence-security structures have acquired a particularly important role.

war no longer begins with the first shot fired on the battlefield, but much earlier through satellite reconnaissance, electronic interception, cyber infiltration, communication analysis, and identification of logistical and command vulnerabilities.

The war in Ukraine clearly demonstrates that classical military doctrine is rapidly evolving into a model of "intelligent warfare," where information, speed of decision-making, technological adaptation, intelligence superiority, and the ability to destroy enemy logistics become more important than sheer manpower and traditional firepower. Future armies will prevail not solely through the strength of weapons, but through the ability to see, understand, process data, and react faster than their opponents.

Economical dimension

The war in Ukraine increasingly underscores a fundamental transformation in the economics of warfare, characterized by the emergence of an economy-of-force model in which relatively inexpensive, autonomous, and semi-autonomous systems generate disproportionately high strategic, operational, and tactical effects against significantly more expensive conventional military assets. The traditional relationship between military investment and battlefield effectiveness is being fundamentally redefined. Systems such as FPV drones, loitering munitions, autonomous reconnaissance platforms, and AI-assisted targeting tools can be produced, deployed, and replaced at a fraction of the cost required for modern tanks, armored vehicles, combat aircraft, air-defense systems, or naval platforms. Despite their relatively low cost, these systems have repeatedly demonstrated the ability to destroy, disable, or degrade military assets worth millions of dollars, thereby altering the economic logic that has traditionally governed military power and force structure planning.

This transformation is creating a new battlefield environment in which operational success is increasingly determined not by the absolute value of military hardware, but by the ability to achieve favorable cost-exchange ratios. A drone costing only a few hundred dollars can destroy a

multimillion-dollar tank. At the same time, coordinated swarms of inexpensive unmanned systems can compel an adversary to expend highly sophisticated and costly air-defense missiles. As a result, military effectiveness is no longer measured solely by the quantity of heavy equipment, manpower, or defense spending, but increasingly by the capacity to integrate affordable technologies into highly adaptive combat networks capable of generating strategic effects disproportionate to their financial cost.

The Ukrainian experience demonstrates that modern warfare is entering an era in which technological adaptability, innovation, rapid production cycles, and efficient resource utilization may generate greater combat effectiveness than traditional mass and firepower alone. This shift represents not merely a technological evolution but a profound transformation in the economics of warfare itself. Victory increasingly belongs to the side capable of maximizing operational impact while minimizing resource expenditure and simultaneously imposing unsustainable military and economic costs upon its adversary. In this emerging model, the ability to achieve strategic paralysis through relatively inexpensive technological means may prove more decisive than the traditional accumulation of heavy weaponry and conventional combat power.

Artificial Intelligence as a Battlefield Multiplier

The war in Ukraine demonstrates that Artificial Intelligence (AI) is rapidly becoming one of the most important force multipliers in modern warfare. While drones, electronic warfare systems, and precision-guided weapons often receive the greatest public attention, their effectiveness increasingly depends on the ability to collect, process, analyze, and distribute vast amounts of battlefield data in real time.

AI enables military forces to transform information superiority into operational superiority by accelerating decision-making, improving target identification, optimizing resource allocation, and enhancing battlefield awareness. Traditionally, military commanders relied on lengthy intelligence cycles involving reconnaissance, analysis, planning, and execution. In modern combat environments, however, the volume of available information exceeds human operators' ability to process it effectively.

Thousands of drones, satellites, reconnaissance sensors, intercepted communications, radar systems, and open-source intelligence platforms generate enormous amounts of data every hour. AI systems increasingly perform filtering, prioritization, and analysis of this information, allowing commanders to identify threats and opportunities far more rapidly than would otherwise be possible. One of the clearest examples can be observed in Ukrainian drone operations. FPV drones themselves are not inherently revolutionary technologies. Their true effectiveness emerges when integrated into a broader digital ecosystem that combines reconnaissance data, satellite imagery, target databases, electronic Intelligence, and AI-supported analytics. Before an attack, AI-assisted systems can compare newly collected imagery with historical data, identify changes in enemy positions, detect vehicle concentrations, locate ammunition depots, and highlight logistical activity. This significantly reduces the time required to identify targets and prepare strikes. Artificial Intelligence also plays an increasingly important role in target recognition and battlefield surveillance. Modern machine-learning algorithms can analyze drone footage and automatically distinguish between tanks, armored personnel carriers, artillery systems, trucks, radar installations, and civilian vehicles. Instead of requiring operators to review hours of video recordings manually, AI systems can automatically flag potential targets for human review. This dramatically increases operational tempo while reducing the workload on intelligence personnel.

The Ukrainian battlefield has also demonstrated the growing importance of AI in counter-battery warfare. Modern artillery engagements increasingly resemble a competition between sensors and algorithms. When enemy artillery fires, drones, acoustic sensors, radar systems, and electronic intelligence assets immediately begin collecting data. AI-assisted systems can rapidly calculate the probable location of firing positions, prioritize targets, and recommend optimal responses. This significantly reduces the time between detection and engagement, increasing the survivability of friendly forces while decreasing the effectiveness of enemy artillery.

A particularly important area of AI application involves the protection of logistical networks. Since logistics has become the primary target of modern warfare, military planners increasingly rely on advanced analytics to predict threats against supply routes, ammunition depots, fuel

distribution systems, and transportation corridors. AI can analyze patterns of enemy drone attacks, identify vulnerable sectors, forecast likely strike locations, and recommend alternative supply routes. In this way, AI contributes not only to combat operations but also to sustaining operational endurance. The Ukrainian experience further demonstrates how AI can support electronic warfare and counter-drone operations.

Modern electronic warfare systems increasingly employ machine-learning algorithms that can identify communication patterns, detect drone-control frequencies, classify threats, and adapt jamming techniques in real time. This creates a dynamic digital battlefield where both sides continuously compete for control of information and electromagnetic space. Perhaps the most significant contribution of AI lies in accelerating the military decision-making cycle. Classical military theory emphasizes the importance of completing the Observe–Orient–Decide–Act (OODA) cycle faster than the opponent. AI directly enhances each phase of this process. It enables faster observation through automated sensor analysis, more accurate orientation through predictive analytics, improved decision-making through real-time recommendations, and more effective action through integrated command-and-control systems. The side capable of processing information and making decisions more rapidly increasingly gains a decisive operational advantage.

The war in Ukraine suggests that future military success will depend not only on the quantity of troops, tanks, artillery systems, or drones, but increasingly on the ability to integrate Artificial Intelligence into a unified digital combat architecture. AI is gradually evolving from a supporting technology into a central component of modern military power. As warfare becomes increasingly data-driven, the ability to collect, process, analyze, and exploit information faster than the adversary may become as important as traditional firepower itself. In this emerging model of intelligent warfare, information processing speed, algorithmic superiority, and decision-making efficiency are becoming critical determinants of battlefield success.

From Kill Chain to Kill Web: The Networked Battlefield

The war in Ukraine underscores a fundamental transformation in the way modern military forces identify, track, engage, and destroy targets. For decades, military operations were largely based on the concept of the Kill Chain, a linear process in which a target is detected, identified, tracked, engaged, and assessed following a relatively sequential series of actions. This model was highly effective in conventional warfare, where information flowed through hierarchical command structures and battlefield dynamics evolved slowly.

However, the operational realities of Ukraine increasingly reveal the limitations of this approach. Modern warfare is evolving toward a far more dynamic and interconnected model known as the Kill Web, where multiple sensors, intelligence platforms, weapons systems, and command networks operate simultaneously as an integrated combat ecosystem. In a traditional Kill Chain, a reconnaissance asset identifies a target, intelligence personnel verify the information, commanders approve engagement, and a designated weapon system executes the strike. Each stage depends upon the successful completion of the previous one. Such a model creates vulnerabilities because the disruption of any single link can interrupt the entire process.

The Ukrainian battlefield has shown that modern combat requires far greater speed, flexibility, redundancy, and adaptability than traditional linear systems can provide. The Kill Web concept replaces this linear structure with a distributed network of interconnected capabilities. Satellites, reconnaissance drones, FPV drones, electronic warfare systems, cyber assets, artillery units, intelligence services, airborne sensors, and command centers continuously exchange information in real time. Rather than relying on a single pathway from detection to engagement, multiple pathways simultaneously contribute to target acquisition and strike execution. If one sensor is lost or one communication channel is disrupted, alternative nodes within the network continue to

support the operation. The Ukrainian use of drones provides one of the clearest examples of Kill Web warfare in practice.

A reconnaissance drone may identify a Russian ammunition depot. The imagery is immediately transmitted through digital networks to intelligence analysts, AI-assisted target recognition systems, artillery command centers, and nearby FPV drone operators. Simultaneously, electronic warfare assets monitor Russian communications while satellite imagery provides additional confirmation of target activity. Within minutes, artillery units, loitering munitions, or FPV drones can engage the target based on a common operational picture shared across multiple platforms. No single system conducts the operation independently; instead, success results from the integration of numerous interconnected capabilities functioning as a unified combat network. The destruction of Russian logistics during Ukrainian operations in 2026 illustrates this principle particularly well. Ukrainian forces frequently combined satellite reconnaissance, drone surveillance, electronic Intelligence, precision artillery, and FPV drone attacks against logistical convoys and supply hubs. Reconnaissance drones identified vehicle movements, electronic warfare systems intercepted communications, intelligence units analyzed logistical patterns, and artillery systems conducted precision strikes. FPV drones then exploited the resulting confusion to destroy surviving vehicles and disrupt recovery efforts. Each component reinforced the effectiveness of the others, producing operational effects far greater than any individual capability could achieve independently. Electronic warfare represents another critical component of the Kill Web architecture. Modern military networks depend heavily on communication systems, navigation signals, data links, and digital command structures. Ukrainian operations have repeatedly highlighted how electronic warfare can isolate enemy units from the broader battlefield network. Once communications are disrupted, artillery units lose targeting information, logistics convoys lose coordination, drones lose guidance links, and commanders lose situational awareness. In network-centric warfare, destroying information connectivity can be as effective as destroying physical assets.

Artificial Intelligence increasingly serves as the connective tissue of the Kill Web. Modern combat generates enormous volumes of data from drones, satellites, sensors, intelligence reports,

and battlefield communications. AI-assisted systems help process this information, identify patterns, prioritize targets, and distribute actionable Intelligence throughout the network. Rather than replacing human decision-makers, AI accelerates the flow of information and shortens the time between detection and engagement. This allows military forces to complete decision cycles faster than their opponents and maintain a persistent operational advantage.

The war in Ukraine further suggests that the effectiveness of the Kill Web depends not only on technology but also on organizational adaptation. Small tactical units equipped with drones, secure communications, and access to real-time Intelligence can now generate effects previously achievable only by much larger formations. Battlefield success increasingly depends upon the ability to connect sensors, shooters, intelligence assets, electronic warfare systems, and decision-makers into a unified operational network capable of functioning under conditions of constant disruption.

The emergence of the Kill Web represents one of the most significant transformations in military affairs since the advent of precision-guided munitions. Future wars are likely to be decided not by the side possessing the largest number of tanks, aircraft, or artillery systems, but by the side capable of creating the most resilient, adaptive, and integrated combat network. In this new model of warfare, military power is increasingly measured by the ability to connect information, Intelligence, decision-making, and firepower into a seamless operational architecture that can observe, understand, decide, and act faster than the adversary.

Digital Battlefield Performance Systems and the Data-Driven Military

One of the least discussed but potentially most revolutionary lessons emerging from the war in Ukraine is the growing use of digital battlefield performance management systems to evaluate combat effectiveness, allocate resources, and incentivize operational success. Traditionally, military organizations relied on hierarchical reporting structures, subjective assessments, and bureaucratic decision-making processes to determine the distribution of equipment, ammunition, funding, and operational priorities.

The Ukrainian experience increasingly suggests a transition toward a data-driven military model in which battlefield performance can be measured, analyzed, and rewarded in near real time. A notable example is Ukraine's implementation of digital performance evaluation mechanisms such as the ePoints system, which seeks to quantify battlefield results through objective operational indicators.

Under this approach, military units receive credit for verified combat achievements, including the destruction of enemy equipment, successful reconnaissance missions, target identification, drone strikes, and other measurable operational contributions. These achievements are digitally recorded, verified through battlefield intelligence and drone footage, and incorporated into centralized databases that support decision-making on resource and capability allocation.

This represents a significant departure from traditional military management practices. Historically, resource allocation often depended on pre-war organizational structures, command influence, bureaucratic procedures, or periodic assessments that could not fully capture rapidly changing battlefield realities. In contrast, digital performance systems create a mechanism for directing resources to units that consistently deliver operational results. Commanders gain access to more accurate information regarding the effectiveness of subordinate formations, while military planners can identify successful operational practices and replicate them across the force. The Ukrainian battlefield provides numerous examples of how such systems can influence operational effectiveness. Drone units that successfully identify and destroy enemy artillery systems, ammunition depots, command posts, or logistical convoys generate measurable battlefield effects that can be documented through digital evidence. These results may then justify the allocation of additional drones, electronic warfare equipment, communications systems, or training resources to the most effective units. In this way, operational success directly influences future combat capability.

The integration of digital performance metrics also supports a broader transformation toward evidence-based military management. Modern warfare increasingly generates enormous quantities of operational data through drones, satellites, sensors, communications networks, and intelligence platforms. By combining this information with digital evaluation systems, military organizations can move beyond subjective reporting and develop more accurate assessments of

combat effectiveness. Such systems provide commanders with a clearer understanding of which tactics, technologies, and organizational structures produce the best battlefield outcomes. Artificial Intelligence is likely to play an increasingly important role in this process.

As the volume of combat data continues to grow, AI-assisted analytics can help identify patterns of success and failure across multiple units and operational environments. Commanders may eventually gain access to predictive assessments that recommend optimal resource allocation, identify emerging operational weaknesses, and forecast future battlefield requirements. This would further enhance the speed and accuracy of military decision-making. The significance of these developments extends beyond Ukraine.

The emergence of digital battlefield performance systems suggests that future military organizations may increasingly resemble highly adaptive data-driven institutions rather than traditional bureaucratic structures. Combat effectiveness will no longer be assessed solely through periodic evaluations or senior command judgments, but through continuous measurement of operational outcomes supported by digital evidence and advanced analytics. The war in Ukraine therefore indicates that the future battlefield will not only be shaped by drones, artificial Intelligence, electronic warfare, and precision weapons, but also by the ability to collect, verify, analyze, and exploit operational data. Military success will increasingly depend upon the capacity to transform battlefield information into actionable knowledge, allocate resources based on measurable performance, and continuously adapt organizational structures to evolving combat realities. In this emerging model of warfare, data itself becomes a strategic resource, and the ability to manage it effectively may prove as important as the ability to employ military force.

Logistics Attrition Warfare: The Emergence of a New Operational Paradigm

One of the most significant lessons emerging from the war in Ukraine is the growing importance of what may be described as *Logistics Attrition Warfare*. Unlike traditional forms of warfare, where military success is primarily achieved through the direct destruction of enemy combat forces and the seizure of territory, this emerging model focuses on systematically degrading the adversary's logistical, informational, and command infrastructure until operational paralysis

ensues. The objective is not necessarily to destroy every enemy unit on the battlefield, but to render those units incapable of sustaining effective combat operations. Historically, military campaigns often sought decisive victories through the destruction of enemy armies in major battles.

From the Napoleonic Wars to the large-scale mechanized offensives of the twentieth century, military doctrine emphasized concentration of force, territorial breakthroughs, and the physical defeat of opposing formations. While logistics has always played a critical role in warfare, it was generally viewed as a supporting function rather than the primary operational objective. The war in Ukraine increasingly suggests that this relationship is changing fundamentally.

The Ukrainian battlefield has repeatedly shown that modern military forces can suffer operational defeat long before they experience catastrophic battlefield losses. Units deprived of ammunition, fuel, spare parts, communications, intelligence support, and logistical resupply gradually lose combat effectiveness regardless of their numerical strength or defensive positions. Deep trench systems, fortified bunkers, minefields, and extensive defensive belts provide limited protection when the logistical systems supporting them are systematically disrupted.

A clear example can be observed in Ukrainian operations targeting Russian ammunition depots, fuel storage facilities, railway infrastructure, bridges, logistical convoys, and command centers. Rather than focusing exclusively on frontline engagements, Ukrainian forces increasingly sought to attack the systems that allowed Russian units to continue fighting. FPV drones, long-range strike systems, artillery, special operations forces, cyber capabilities, and intelligence assets were employed not only to destroy enemy troops, but also to disrupt the continuous flow of resources required to sustain military operations. Once logistical networks were disrupted, frontline units often became isolated, vulnerable, and increasingly unable to coordinate resistance.

The significance of this approach becomes particularly evident when examining the relationship between logistics and operational tempo. Modern warfare consumes enormous quantities of ammunition, fuel, spare parts, communications equipment, and technical support. Armored formations, artillery systems, air-defense networks, and drone units all depend upon continuous resupply. Even highly capable military formations can rapidly lose effectiveness when logistical support is interrupted. The side capable of disrupting enemy sustainment systems while

preserving its own gains a decisive operational advantage regardless of the balance of forces at the frontline.

The emergence of drones has dramatically accelerated this transformation. Previously, attacking logistical targets deep behind enemy lines often required expensive aircraft, cruise missiles, or special operations forces. Today, relatively inexpensive FPV drones, loitering munitions, and long-range unmanned systems can continuously threaten fuel convoys, supply depots, command posts, transportation hubs, and maintenance facilities.

The result is a battlefield where logistics itself becomes permanently exposed to attack. Supply routes that once operated relatively safely behind the front are now part of the active combat zone. Artificial Intelligence, satellite reconnaissance, electronic warfare, and real-time intelligence sharing further strengthen the effectiveness of Logistics Attrition Warfare. Modern sensors can identify logistical patterns, track vehicle movements, detect supply concentrations, and reveal vulnerabilities within transportation networks. AI-assisted analytics can help prioritize targets and predict future logistical activity, allowing military planners to focus strikes where they will generate the greatest operational disruption. The objective is not merely destruction, but the systematic erosion of the enemy's ability to sustain military operations over time.

The Russian-Ukrainian conflict also demonstrates that Logistics Attrition Warfare extends beyond purely military targets. Energy infrastructure, transportation systems, communications networks, industrial production facilities, and digital infrastructure increasingly influence a state's ability to sustain prolonged conflict. Modern warfare therefore involves the contestation of entire support ecosystems rather than merely battlefield formations. Military power is increasingly dependent upon the resilience of national logistical and industrial systems operating far beyond the immediate combat zone.

For this reason, Logistics Attrition Warfare may represent one of the defining characteristics of twenty-first-century conflict. Victory is no longer determined solely by territorial conquest or the destruction of enemy combat units. Instead, success increasingly depends upon the ability to systematically degrade the adversary's operational metabolism while preserving one's own capacity for sustainment and adaptation. The side capable of maintaining continuous logistical

flow, information superiority, and operational resilience while simultaneously disrupting the enemy's sustainment network gains a decisive strategic advantage.

The war in Ukraine suggests that future military campaigns may increasingly resemble contests of systemic endurance rather than traditional battles of annihilation. In this emerging operational paradigm, logistics is no longer merely a supporting function of warfare—it becomes one of its primary centers of gravity. The ability to identify, target, disrupt, and destroy the systems that sustain military power may prove more decisive than the direct destruction of combat forces themselves. As a result, Logistics Attrition Warfare is emerging as a distinct model of modern conflict, reflecting the broader transition from industrial-age warfare toward networked, information-driven, and technologically integrated forms of military competition.

Слава України! Слава херојима! (Glory to Ukraine)

Ukraine may ultimately be remembered as the conflict that marked the transition from industrial-age warfare to intelligent warfare. Future military success will increasingly depend not on the mass of forces deployed, but on the ability to disrupt, paralyze, and out-adapt the enemy's operational ecosystem. Perhaps the most remarkable strategic lesson of the war is the transformation of Ukraine itself. In 2022, Ukraine was widely perceived as the weaker party confronting what was then considered the world's second or third most powerful military force. Four years later, Ukraine has evolved into one of the most capable and combat-experienced military powers on the European continent.

Through continuous adaptation, innovation, and battlefield learning, Ukrainian forces have developed expertise in drone warfare, electronic warfare, networked operations, logistics interdiction, and AI-supported military decision-making that few European armies currently possess. At the same time, the defense of Europe against Russian offensive activities may only be entering its initial phase. While many European states have begun to recognize the scale of the Russian challenge and have initiated significant rearmament programs, the broader strategic contest extends far beyond conventional military power.

The war in Ukraine has demonstrated that modern competition involves intelligence operations, cyber activities, information warfare, political influence networks, economic pressure, and long-term strategic penetration of institutions and societies. The collapse of the Soviet bloc did not automatically eliminate all structures, networks, and operational cultures developed during the Cold War. Elements of former intelligence, security, political, and influence networks survived in various forms across Europe, creating opportunities for continued Russian influence and intelligence activity. The persistence of these legacy structures, combined with modern cyber and information capabilities, represents a long-term security challenge that European states are only beginning to address. The future security of Europe will therefore depend not only on rebuilding military capabilities, but also on strengthening societal resilience, counterintelligence capacities, cyber defenses, critical infrastructure protection, and strategic awareness. The lessons of Ukraine suggest that future conflicts will be decided as much by the ability to defend information space, institutions, and national resilience as by success on the battlefield itself.

Ukraine represents the largest kinetic target of contemporary Russian offensive action in Europe. Since 2022, the country has been exposed to a combination of conventional military operations, missile attacks, drone warfare, cyber operations, economic pressure, and information campaigns aimed at weakening its capacity for resistance and state resilience. The Ukrainian battlefield has become the principal testing ground for new concepts of warfare and the central arena of Russia's effort to revise the European security order through military force.

At the same time, Serbia has emerged as one of the most significant targets of Russian hybrid influence operations in Europe. Unlike Ukraine, where military force represents the primary instrument of pressure, Russian activities in Serbia are predominantly conducted through information operations, political influence networks, intelligence activities, economic leverage, media penetration, historical narratives, religious connections, and the exploitation of existing social and political divisions. The objective is not territorial conquest but strategic influence, political dependency, societal polarization, and the limitation of Serbia's independent strategic decision-making.

The contrast between Ukraine and Serbia illustrates two complementary dimensions of contemporary Russian strategy. Ukraine faces the kinetic dimension of Russian power, while Serbia is exposed primarily to its hybrid dimension. Both forms of pressure ultimately pursue the same strategic objective: the expansion of Russian influence and the weakening of Western political, security, and institutional presence in Eastern and Southeastern Europe.

The lessons of Ukraine therefore extend far beyond the battlefield. They demonstrate that future conflicts will not be fought exclusively through military force but through a combination of kinetic operations, intelligence activities, cyber campaigns, information warfare, political influence, economic pressure, and strategic manipulation of social perceptions. In this broader context, strengthening national resilience becomes as important as strengthening military power itself.