INSIGHT PAPER / STRATEGIC ASSESSMENT

Making the Battlefield Lie

How Armies Get Manoeuvre Back in the Age of Persistent Observation

Battlefield Transparency, Decision Denial and the Return of Operational Manoeuvre

CENTRAL ASSESSMENT

Manoeuvre warfare is not dead. What has disappeared is the assumption that forces can concentrate and move while an enemy reconnaissance-strike system functions uninterrupted. Armies regain manoeuvre by degrading, confusing and delaying the enemy's ability to turn observation into action long enough to create local windows of opacity. The objective is not permanent invisibility; it is to make the enemy wrong for long enough to move.

ADG CONSULT NZ

SEPTEMBER 2026

INSIGHT PAPER / STRATEGIC ASSESSMENT

Executive Assessment

This Insight Paper is deliberately structured for two levels of readership. The Executive Assessment is designed to stand on its own. A reader who needs the central argument, the principal evidence and the practical implications should be able to stop at the end of this section with a complete understanding of the paper's assessment. The remainder is intended for readers who want to examine the evidence in greater depth, test the argument against different operating environments and consider what the findings imply for doctrine, force design, training and procurement.

The central proposition is that manoeuvre warfare is not dead, but the conditions that once allowed armies to manoeuvre with relative freedom have changed. Against a capable opponent, the ability to concentrate forces, move them at operationally meaningful scale and sustain them while the enemy's reconnaissance and targeting system functions uninterrupted has become increasingly difficult. The proliferation of unmanned aircraft, commercial satellite imagery, electronic sensing, thermal imaging, acoustic detection, digital battle-management systems and precision strike means that movement can generate an observable pattern long before the decisive phase of an operation begins. Ukraine is the clearest contemporary demonstration of this problem, but it should not be mistaken for a universal template for every future battlefield. [1][2]

The useful distinction is between a battlefield that is perfectly transparent and one that is densely observed. Perfect transparency would imply that everything can be seen, correctly identified, continuously tracked and struck in time. No contemporary force possesses that capability. What exists instead is a battlefield in which more activity can be detected, by more kinds of sensors, more frequently and at lower cost than before. That is enough to make early concentration dangerous, to expose logistics and command activity, and to shorten the time available for a force to exploit surprise. It is not enough to eliminate uncertainty. The difference between observation and understanding is therefore the opening through which manoeuvre can return.

Ukraine demonstrates both sides of the problem. The Royal United Services Institute, or RUSI, has documented how persistent intelligence, surveillance and reconnaissance - normally abbreviated ISR - makes surprise more difficult and allows defenders to answer concentrations of force with concentrations of effects. ISR in this context means the sensors, people and systems used to discover what an opponent is doing, maintain awareness of it and pass that information to commanders or weapons. RUSI also describes higher-performing Ukrainian formations deliberately attacking enemy reconnaissance, electronic-warfare systems and supporting fires before committing assault forces, then exploiting weather, thermal crossover and local gaps in sensor coverage to create more favourable conditions for movement. The evidence therefore does not support the simplistic conclusion that manoeuvre has disappeared. It supports a more demanding conclusion: armies increasingly have to earn the right to manoeuvre. [1]

The paper develops two analytical concepts to explain what that means. These are not presented as established NATO or U.S. doctrinal terms. The first is decision denial. Decision denial means preventing an adversary from converting what it can observe into sufficiently reliable and timely understanding to act effectively. A sensor may function perfectly while the wider system still fails if the target is misidentified, the information arrives too late, communications are interrupted, weapons are unavailable or deception causes the enemy to allocate effort to the wrong place. The second concept is the window of opacity. A window of opacity is a temporary and geographically limited period in which the opponent's understanding of a particular part of the battlefield becomes incomplete, delayed or sufficiently uncertain that manoeuvre becomes possible. Opacity does not mean invisibility. It means that what is visible cannot be converted into confident action quickly enough.

This distinction changes how anti-access and area-denial problems should be understood. Anti-access/area denial, usually written A2/AD, describes capabilities intended to prevent an opposing force entering an area or to restrict its freedom of action once inside it. Modern A2/AD can make particular airspace, waters or ground corridors prohibitively dangerous for high-value crewed platforms. Yet physical denial does not necessarily produce information denial. Commercial satellites can observe from outside the defended airspace. Cheap drones can be sent repeatedly into an area even when losses are expected. Autonomous underwater vehicles can survey dangerous waters. Unattended sensors can remain after the force that emplaced them has withdrawn. If the adversary is prevented from placing a crewed reconnaissance aircraft over a target but still maintains target-quality understanding through other means, the defended territory is denied in one sense and not in another.

The economics of attritable systems deepen the problem. In defence terminology, an attritable platform is not a system intended to be thrown away casually. It is a system designed and priced so that commanders can accept a higher probability of loss than they could for scarce, exquisite or crewed platforms. The U.S. Department of Defense used this logic in the Replicator initiative, which sought large numbers of autonomous systems across multiple domains and explicitly described such systems as affordable enough to employ at greater risk. The 8 September 2026 capture by Iran of a U.S. Dive-LD autonomous underwater vehicle near the Strait of Hormuz is a contemporary illustration. The Pentagon confirmed that the vehicle had malfunctioned during survey activity, while manufacturer Anduril emphasised that the system was designed for difficult missions in which losses are anticipated. The strategic effect of losing such a vehicle is not equivalent to the loss of a crewed submarine or an expensive intelligence aircraft. [5][6]

The same logic applies to the sensor-to-shooter chain. The phrase describes the sequence through which a force detects something, identifies and locates it, passes the information to a decision-maker, allocates a weapon and engages the target. Modern digital networks can compress this sequence dramatically. U.S. Army analysis of lessons from Ukraine describes targeting cycles as short as several minutes in some circumstances, while CSIS has documented Ukraine's use of commercial satellite imagery delivered directly to operators to support a strike on Russian Shahed-launch infrastructure at occupied Donetsk Airport in June 2026, with coordinates reportedly reaching operators about fifteen minutes after collection. The significant development is not simply that satellites can see military activity. It is that space-based observation can increasingly be connected directly to tactical action. [3][4]

This does not mean that manoeuvre is obsolete. It means that the old sequence of concentrating, breaching, manoeuvring and exploiting may expose the operation too early if concentration itself reveals intent. A future sequence is more likely to keep forces dispersed for longer, map and attack the enemy reconnaissance system, create false indicators, suppress or corrupt selected sensors, exploit terrain and weather, concentrate only when the local information environment has been shaped, manoeuvre through the resulting opening, and disperse again before the enemy reconstructs an accurate picture. The battle for perception therefore moves ahead of the decisive movement.

The analogy with suppression of enemy air defences is useful. Suppression of enemy air defences, normally abbreviated SEAD, does not require every hostile radar and missile system to be permanently destroyed before aircraft operate. It seeks to suppress, disrupt, deceive or destroy enough of the air-defence network, in the relevant place and for the required period, to create a usable corridor. Ground forces increasingly need an analogous approach to hostile reconnaissance. This paper uses the descriptive phrase Suppression of Enemy Reconnaissance for that function: the coordinated destruction, disruption and deception of the sensors, operators, communications links, processing systems and strike relationships that allow an opponent to turn observation into effects. The purpose is not to eliminate observation across an entire theatre. It is to create a local information advantage at the decisive point.

Geography determines how difficult this will be. Ukraine contains extensive open agricultural terrain, developed road networks and many sectors in which aerial observation is unusually effective. A Southeast Asian jungle battlefield would behave differently. U.S. jungle doctrine describes severely restricted observation, difficult movement and the disproportionate importance of roads, waterways, crossing points and landing zones. Dense canopy can degrade direct optical observation and complicate radio links, while rain, humidity and vegetation change the performance of both people and equipment. Jungle therefore returns some concealment but removes mobility. A small unit may move under canopy with much less exposure than a formation crossing open Ukrainian farmland, while a brigade still has to move fuel, ammunition, vehicles and communications through a limited number of roads, rivers, bridges, ports and clearings. The sensors do not disappear; they migrate toward the places where movement becomes unavoidable. [10]

The broader implication is that future battlefields should be understood as mosaics of transparency and opacity rather than as uniformly transparent spaces. A coastline can be heavily observed while jungle immediately inland is comparatively concealed. A road emerging from that jungle can again become transparent. A city can produce enormous visual, thermal and electronic clutter while a bridge within it becomes one of the most watched points in the theatre. Weather can reduce some drone performance for hours. Electronic warfare can make one area difficult for radio-controlled systems while leaving fibre-optic or autonomous systems less affected. Commanders who understand this changing sensor geography can use it in the same way earlier commanders used dead ground, reverse slopes, darkness and weather.

Deception becomes central because concealment alone is increasingly insufficient. A force that cannot reliably prevent observation can still try to control the conclusion drawn from observation. Modern deception must therefore be multispectral and behavioural. Multispectral means that a false target must look plausible across several forms of sensing: visual imagery, thermal signatures, radar returns and electronic emissions. Behavioural means that the pattern around the target must also make sense. A false command post may need realistic radio activity. A decoy missile battery may need support vehicles and heat. A false crossing may require visible engineering preparation. The objective is not merely to hide the real force but to create a coherent false explanation that competes with the truth.

This produces the paper's most provocative conclusion. A military can control territory, control the airspace above it and destroy hostile platforms entering it, yet still fail to deny the enemy the battlespace if the enemy can continue to observe, understand and generate effects. Conversely, an attacking force may not need to blind every sensor to regain manoeuvre. It may need only to make the defender wrong for long enough. If a formation requires forty-five minutes to cross a vulnerable area, a forty-five-minute period of uncertainty may have operational value even if the enemy's ISR network eventually recovers.

Armies therefore get manoeuvre back by treating the enemy's perception of the battlefield as something that can be attacked. Counter-ISR becomes a manoeuvre function rather than merely force protection. Electronic warfare must be synchronised with movement rather than applied indiscriminately. Signature management becomes ordinary fieldcraft. Deception becomes part of every major operation rather than a specialist annex. Weather and terrain become elements of sensor planning. Commanders must understand how long an opponent takes to reconstruct its picture after sensors are destroyed, jammed or deceived. Procurement must favour not only high-end platforms but also inexpensive sensors, interceptors, decoys and software that can be altered quickly as the enemy adapts.

The conclusion is not that technology restores a romantic form of free manoeuvre or makes the battlefield of 2026 resemble the battlefield of 1991. Minefields, artillery, precision strike, autonomous systems and persistent sensing will continue to impose severe constraints. Manipulating transparency creates opportunity; it does not guarantee success. Combined arms, logistics, leadership, training, morale and geography remain decisive. What changes is the price of admission. Future formations may have to win a local contest over perception before they can win the physical contest over terrain.

Manoeuvre warfare survives because its underlying purpose is not movement for its own sake. It is to create surprise, tempo, dislocation and a situation the opponent cannot solve quickly enough. Those principles remain viable if armies can impose temporary information asymmetry - understanding enough about the enemy while preventing the enemy from understanding them with equal speed and confidence. The battlefield of the future may be impossible to hide, but it may still be possible to make it lie.

1. Introduction: The Question Is Not Whether Armies Can Be Seen

Debate over the future of manoeuvre warfare is often framed too absolutely. One side points to the proliferation of drones, commercial satellites and precision strike and concludes that large formations can no longer move without being destroyed. The other points to historical examples of military adaptation and argues that every apparent technological revolution is eventually absorbed into combined arms. Both positions contain part of the truth. The contemporary battlefield has become much more observable, and that observability has imposed real constraints on concentration and movement. At the same time, observation is not understanding, and understanding is not instantaneous lethality. The practical problem is therefore not whether armies can avoid being seen altogether. It is whether they can control the quality and timing of the enemy's understanding sufficiently to create opportunities for decisive movement.

This distinction matters because manoeuvre warfare has never depended on literal invisibility. Surprise can concern time, direction, scale, method or purpose. An opponent may know that an attack is likely while remaining uncertain where the main effort will fall. It may observe vehicles moving without knowing whether they belong to the attacking force, a reserve, a deception plan or routine logistics. It may correctly identify an assembly area but misjudge when the attack will begin. Military history is full of operations in which important activity was observed yet incorrectly interpreted. What changes in the contemporary environment is the amount of information available and the speed with which that information can be fused and acted upon.

The U.S. Department of Defense has summarised the new pressure in blunt terms: if a force can be seen, it can be hit. The statement is useful because it forces armies to take signature management seriously, but it becomes misleading if treated as a physical law. Detection still has to be converted into identification, location, tracking, decision, weapon allocation, engagement and assessment. Every link can fail or be delayed. Modern warfare is therefore increasingly a contest over the integrity and speed of that chain. [2]

The argument of this paper is that the return of manoeuvre depends upon exploiting those imperfections deliberately. Armies cannot assume a sanctuary exists simply because a location is behind the front, under friendly air defence or geographically remote. Nor should they conclude that the only answer is permanent dispersal and attrition. A force that remains dispersed forever may survive but cannot necessarily create decisive local superiority. Manoeuvre requires concentration at some point. The operational art lies in determining how late that concentration can occur, how quickly it can be created, how long it can be sustained and what must happen to the enemy's reconnaissance system before the force is exposed.

2. The Battlefield Is Densely Observed, Not Perfectly Transparent

The phrase transparent battlefield is now common, but it should be used carefully. Transparency suggests that the battlefield can be seen through as if nothing is hidden. Contemporary forces do not possess that level of knowledge. What they possess is a dense and overlapping collection environment. Small unmanned aircraft can provide persistent local observation. Longer-range drones can watch routes and rear areas. Commercial satellites can provide optical or radar imagery at intervals that were once available only to a small number of states. Signals intelligence can detect and locate some electronic emissions. Thermal sensors reveal heat. Acoustic arrays can detect engines, artillery and unmanned aircraft. Human reporting, open-source imagery and digital communications add further layers.

The significance is cumulative. A single sensor may be unreliable. Several independent-looking sensors can reinforce one another and create confidence. A vehicle park detected by satellite may later be seen by a drone. Increased radio traffic may suggest a headquarters has become active. Fuel vehicles may move toward the same sector. Engineers may begin work on a crossing. No individual observation proves an attack is imminent, but the pattern can reveal preparation. This is why the transparency problem begins before the first assault element crosses a line of departure.

Commercial space has become particularly important because access is broader and observation can be repeated more frequently than in earlier conflicts. More military users can obtain useful satellite imagery, from more commercial providers, with shorter intervals between observations than was historically possible. In June 2026, CSIS reported that Ukrainian forces used commercial satellite imagery delivered directly to operators to support an attack on Shahed-launch infrastructure at occupied Donetsk Airport. Coordinates were reportedly available about fifteen minutes after collection. The development demonstrates how a strategic sensing layer can increasingly feed tactical action without a long headquarters process. [3]

The same compression is visible closer to the front. U.S. Army analysis published in July 2026 described the Ukrainian battlespace as one in which targets may be prosecuted within only a few minutes of detection in some circumstances. The Army paper focused on communications survivability, but the implication is wider: equipment that emits, remains stationary or behaves predictably can become part of an adversary's target-development process very quickly. [4]

Yet the density of observation should not be confused with certainty. Sensors have blind spots. Weather interferes. Trees, buildings, terrain and distance block or distort observation. Radio-frequency detection can reveal that something is transmitting without necessarily establishing what it is. Thermal systems can detect heat without proving the identity of the source. Radar can see movement or structure without resolving intent. Analysts can misinterpret data. Automated classification can be wrong. A force can therefore accept that observation is persistent while still contesting what the observation means.

Tactical UAV operations in Ukraine. A Ukrainian soldier launches a small unmanned aerial vehicle from a concealed position. The image illustrates how low-cost, rapidly deployable drones have pushed reconnaissance and surveillance capabilities down to tactical level, reducing the ability of forces to move or concentrate without observation.

3. Movement Has Become a Signature Before It Becomes a Manoeuvre

One of the most consequential changes is that preparations for movement increasingly generate signatures of their own. A major offensive does not begin when the first vehicle advances. It begins much earlier in fuel distribution, ammunition movement, reconnaissance, engineering preparation, medical planning, air-defence repositioning, command activity and reserve management. Each activity can create visual, thermal, electronic or behavioural indicators. The larger the formation and the longer the preparation, the greater the pattern available to an adversary.

This creates a structural problem for traditional concentration. Combat power is most effective when it can be concentrated at the decisive place. Persistent sensing punishes forces that concentrate too early because the enemy receives time to respond before the attacking force obtains the benefit of its mass. Reserves can be shifted. Additional mines can be laid. Artillery can register likely routes. Drone coverage can be increased. Logistics can be struck. A force may therefore pay the vulnerability cost of concentration without yet receiving the operational benefit.

RUSI's work on Ukrainian combined-arms manoeuvre captures this dynamic. It describes an environment in which reconnaissance and precision fires can make surprise difficult and allow the defender to apply concentrated effects against an attacking formation. It also notes that the problem extends beyond the forward edge of battle. Logistics, artillery and supporting elements remain exposed at increasing depth, limiting the ability to sustain exploitation after an initial success. [1]

This helps explain why the debate about whether tanks or armoured vehicles are obsolete is too narrow. The vulnerability is not unique to a platform. It is attached to detectable behaviour. A tank that moves alone under concealment may survive. A truck convoy that follows a predictable route may not. An artillery battery that fires a few rounds and relocates may survive where a static battery is rapidly targeted. A large headquarters with continuous high-bandwidth communications may become more vulnerable than a small forward element. The battlefield is punishing signatures, routines and time exposed as much as it is punishing particular vehicle types.

4. Denied Territory That Can Still Be Seen

Anti-access and area-denial concepts remain useful because military forces still need to enter and operate in physical space. Anti-access capabilities seek to prevent entry into a theatre or operational area; area-denial capabilities make movement and operations inside that space dangerous or difficult. Long-range missiles, air-defence systems, mines, submarines, coastal weapons, electronic warfare and other systems can all contribute. The conceptual problem arises when the denial of physical presence is assumed to equal the denial of information access.

A high-end air-defence network can make crewed reconnaissance aircraft unwilling to operate over a defended area. That does not prevent a commercial satellite from observing from orbit. A coastal anti-ship system can deter a major surface combatant from approaching a coastline. It does not necessarily prevent an autonomous underwater vehicle from surveying the seabed or a low-cost unmanned surface vessel from attempting to penetrate. A border security system can prevent reconnaissance patrols crossing a frontier while long-range drones and signals intelligence continue collecting from outside it.

The distinction becomes sharper when the observer is expendable or attritable. The 8 September 2026 loss of a U.S. Dive-LD autonomous underwater vehicle near the Strait of Hormuz illustrates the new risk calculus. Iran's Revolutionary Guards announced that they had captured the vehicle. The Pentagon confirmed that a U.S. underwater drone had malfunctioned during survey work and said it carried no classified equipment, while Anduril emphasised that the platform was designed for demanding missions where loss had to be anticipated. The incident still has intelligence and propaganda value for Iran, and it should not be dismissed as costless. Its significance lies in the fact that commanders can place an uncrewed survey system into an environment where they would not accept equivalent risk to a crewed platform. [6]

Attritable autonomous underwater reconnaissance platform. The Dive-LD autonomous underwater vehicle illustrates the growing use of comparatively low-cost, unmanned systems for persistent sensing and survey missions in contested maritime environments. Such platforms complicate traditional concepts of denied territory because access can remain possible for expendable sensors even where risk to crewed or high-value platforms would be unacceptable.

Ukraine's Black Sea operations demonstrate a related separation between presence and effects. Ukrainian unmanned systems have attacked ships, port infrastructure, cranes, substations and other targets associated with Russian maritime logistics without Ukraine possessing conventional sea control in the classic sense. Reuters reported in July

2026 that one Ukrainian drone formation had struck more than 180 vessels and installations during its campaign. This does not mean drones have replaced fleets or that Ukraine controls the Black Sea. It demonstrates that a force can impose military effects inside a space where its conventional presence remains constrained. [7]

The consequence is that denied territory needs a more demanding test. If an adversary cannot safely place people or expensive platforms in an area but can still observe activity, build an accurate picture and generate effects from outside, the area is denied physically but not operationally in the information sense. The question for the defender is therefore not simply whether the opponent can enter. It is whether the opponent can understand what is happening well enough to act.

5. Decision Denial: Attacking the Enemy's Ability to Understand

This paper uses the term decision denial to describe the effort to prevent an adversary from converting available information into sufficiently reliable and timely understanding to support effective action. It is an analytical concept, not a claim that current doctrine uses the term in this exact form. The purpose is to shift attention from individual sensors toward the complete decision system.

A modern reconnaissance-strike system includes detection, identification, location, tracking, communication, processing, command decision, weapon allocation, engagement and assessment. The familiar phrase kill chain is often used for this sequence when the purpose is to destroy a target. Decision denial is wider because military information also supports movement, reinforcement, logistics, deception detection and reserve commitment. An enemy can be denied a useful decision even when no weapon is fired.

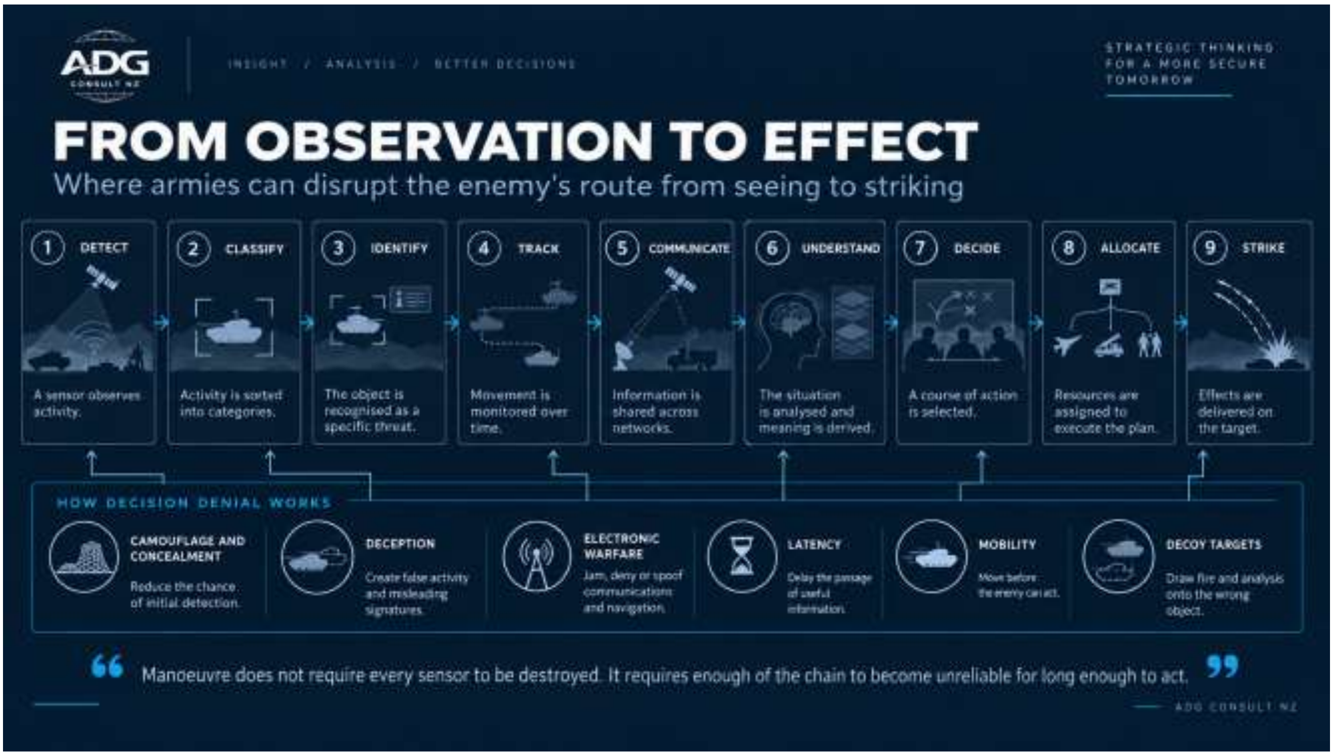

Figure 1. From Observation to Effect: Decision denial can occur at multiple points between initial detection and delivery of battlefield effects.

Consider a drone that correctly detects twenty vehicles. If the operator cannot determine whether they are tanks, trucks or decoys, the picture remains incomplete. If the vehicles are identified but the data cannot be transmitted, the sensor has succeeded while the system has failed. If the information reaches a headquarters but is one of dozens of conflicting reports, decision time increases. If a strike is authorised but the target has already moved, the information was accurate yet operationally stale. If the enemy strikes a decoy formation while the real force moves elsewhere, every technical component may have functioned and the decision can still be wrong.

This is why latency matters. Latency is the delay between one stage of the process and the next. A force that detects a formation and can attack it ninety seconds later presents a very different manoeuvre problem from a force that needs thirty minutes. Both have reconnaissance. Only one has a sufficiently fast reconnaissance-strike relationship to dominate a fleeting movement. Increasing the enemy's latency may therefore be as valuable as reducing its probability of detection.

Decision denial can be produced by kinetic attack, electronic warfare, cyber effects, concealment, deception, terrain, weather and deliberate overload. The most effective method will usually be combined. Destroying a drone may create a small gap. Destroying the operator, disrupting the communications relay and simultaneously presenting false activity may create a larger one. The objective is cumulative uncertainty rather than technical perfection.

6. Attritable Observation Changes the Economics of Denial

Traditional reconnaissance systems were often scarce and expensive. Losing a crewed aircraft, specialised ship or strategic unmanned platform could have large military and political consequences. This encouraged commanders to treat survivability as a central requirement. The rise of cheaper autonomous and semi-autonomous systems changes the relationship between platform loss and mission value.

The Department of Defense's Replicator initiative made the concept explicit. It sought autonomous systems in multiple domains at a scale of thousands and described attritable platforms as affordable enough to allow commanders to accept greater risk. The logic was not that every system should be disposable. High-end platforms remain necessary for missions cheap systems cannot perform. The change is the addition of a large category of systems whose value comes partly from numbers, distribution and replaceability. [5]

This creates difficult defensive economics. A defender that can shoot down seventy-five percent of incoming reconnaissance drones may appear tactically successful. If the attacker can afford to send hundreds and the surviving quarter provide enough information to reveal the main effort, the same engagement may be an operational failure. The relevant metric is no longer only the percentage of platforms destroyed. It is whether the surviving collection was sufficient to support the enemy's decision.

The same problem exists in air defence against one-way attack drones. Russia's increasing use of Shahed-derived Geran systems has repeatedly forced Ukraine to seek cheaper interception methods because using expensive missiles against inexpensive drones is economically unsustainable over time. CSIS estimates that Russia was launching more than 5,000 drones per month on average by early 2026, illustrating the scale at which inexpensive systems can impose continuous defensive costs. [13]

The economic inversion has doctrinal consequences. Counter-reconnaissance cannot rely on exquisite interceptors alone. Armies need layered methods in which inexpensive interceptors, electronic attack, passive detection, camouflage, decoys, mobility and automated warning reduce the need to spend a premium weapon on every cheap sensor. A force that wins each engagement but loses the cost exchange can still be strategically exhausted.

7. Is Manoeuvre Warfare Dead?

The most direct answer is no, but the qualification matters. Unprotected manoeuvre at operationally significant scale may be temporarily untenable against a competent peer whose reconnaissance-strike architecture is functioning well. That is different from saying manoeuvre warfare as an approach to defeating an opponent has become obsolete.

Manoeuvre warfare is often caricatured as armoured formations driving quickly through open terrain. Its underlying logic is broader. Manoeuvre seeks to create surprise, tempo, dislocation and dilemmas, then exploit a weakness before the opposing system can adapt. Physical movement is central, but so are deception, timing, the fixing of enemy forces and the concentration of combat power at a decisive point. Those principles remain valid even when the methods for creating them change.

Ukraine itself provides evidence that manoeuvre remains possible. RUSI's examination of higher-performing Ukrainian formations describes deliberate efforts to survey target sectors, attrit hostile reconnaissance, suppress supporting systems, fix defenders and isolate positions before assault forces are committed. Russian forces have also used small-group infiltration, poor weather and attempts to draw or exhaust Ukrainian drone coverage before committing faster-moving elements. These practices are not a rejection of manoeuvre. They are an attempt to manufacture its prerequisites. [1]

The weather relationship is particularly revealing. In September 2026, analysts cited by Reuters expected deteriorating autumn conditions in Donetsk to reduce some drone effectiveness and potentially allow Russia to attempt renewed mechanised action. Michael Kofman described poor weather as a period when Russian forces often try to return mobility to the battlefield. The observation is important because it shows that manoeuvre has not disappeared; its opportunities are conditional and can expand when sensing temporarily degrades. [14]

A better formulation is therefore that battlefield transparency has removed manoeuvre as the default condition. The force must create or exploit the information conditions that make movement survivable. This is the point at which counter-reconnaissance stops being a supporting activity and becomes part of operational manoeuvre itself.

8. Earning the Right to Manoeuvre

The phrase earning the right to manoeuvre captures a sequencing problem. A force that moves before it has degraded the enemy's ability to understand movement exposes itself to a reconnaissance-strike network at full effectiveness. A force that spends too long shaping the information environment may lose tempo, reveal its preparation or allow the opponent to adapt. The operational problem is therefore to create only as much information advantage as is needed, then exploit it immediately.

The analogy with suppression of enemy air defences is useful because air forces have long accepted that hostile defences cannot always be eliminated permanently. SEAD operations may use anti-radiation weapons, jamming, decoys, cyber effects, route planning and stand-off fires to reduce the effectiveness of an integrated air-defence system for a limited period. Aircraft then exploit the corridor before the network recovers. The objective is sufficient suppression at the decisive time and place, not universal destruction.

Ground forces increasingly require an equivalent mindset toward reconnaissance. The enemy ISR architecture should be mapped as a system. Which drone teams cover the decisive route? Where are their launch points and relays? Which electronic-warfare systems protect them? Which headquarters fuse their reporting? Which fires are normally allocated to the sector? Which commercial or military satellite passes matter during the critical period? Where does terrain block line of sight? Which communications links are fragile? The answer determines what needs to be destroyed, jammed, deceived or simply avoided.

The resulting operation is not an information campaign separate from combat. It is combined arms. Fires may destroy a UAV team. Air defence may intercept higher-altitude reconnaissance. Electronic warfare may delay data links. Engineers may create obscuration or alternative crossings. Infantry may clear observation posts. Cyber or electronic attack may affect networks. Decoys may draw attention toward the wrong axis. The manoeuvre force then moves through the disruption before the adversary reconstructs the picture.

This framing also imposes discipline. The objective is not to chase every drone in the theatre. It is to suppress the sensors that matter to the decision the commander is trying to create. A reconnaissance drone observing an irrelevant sector may be tolerated. A single sensor covering the only bridge needed by the main effort may be decisive. Operational art therefore remains a matter of choice and prioritisation.

9. Suppression of Enemy Reconnaissance

Suppression of Enemy Reconnaissance is used in this paper as a descriptive framework for the coordinated effort to reduce the effectiveness of the enemy's observation and targeting system. It includes more than counter-drone operations. A reconnaissance architecture consists of sensors, operators, launch infrastructure, communications, processing, command relationships and weapons able to exploit the information. Suppression becomes effective when enough of these elements are degraded simultaneously that the enemy cannot maintain a coherent picture.

Kinetic destruction remains important. Drone operators, antenna sites, electronic-warfare vehicles, radars, observation posts and communications relays can all be attacked. But kinetic action alone may produce an endless replacement cycle if the enemy's systems are cheap and numerous. A more sustainable approach combines physical destruction with disruption and deception. A jammed data link may force a drone closer to its operator. A false emitter may cause signals intelligence to search the wrong area. A smoke screen may deny a camera the critical seconds it needs. A decoy can consume an interceptor or artillery mission. Each measure increases friction elsewhere in the system.

The defender faces the same requirement in reverse. Ukraine's experience with Russian fibre-optic FPV drones shows how quickly a successful denial method can be bypassed. Fibre-optic drones transmit control through a physical cable rather than a radio link, making conventional radio-frequency jamming ineffective against the control channel. Reuters documented their use against heavily protected Ukrainian electrical substations, including attacks from around twenty-six kilometres from the front, at a reported cost of roughly $2,000 per drone. The tactical lesson is not that fibre optics defeat all electronic warfare. It is that a defence focused on one technical mechanism can be routed around. [8]

Suppression must therefore target functions rather than individual technologies. If the function is observation, the force may defeat it by destroying the sensor, blocking its view, preventing its data reaching a decision-maker, creating a false target or moving before the information can be acted upon. This functional approach is more resilient because it accepts that the enemy will change hardware while still needing to perform the same underlying tasks.

Training should reflect this reality. Units should be evaluated not only on whether they can shoot down drones but on whether they can create a measurable period in which an enemy reconnaissance network loses confidence. That requires exercises in which the opposing force has realistic sensors, electronic warfare, commercial imagery, decoys and the authority to exploit detected signatures. Without such pressure, forces may practise manoeuvre in an information environment that will not exist in combat.

10. Windows of Opacity

A window of opacity is the practical outcome sought by suppression and deception. The term describes a temporary local condition in which the adversary's picture is too incomplete, delayed or uncertain to support effective action at the required speed. It does not imply that the area becomes invisible. The enemy may still collect fragments. The operational value lies in preventing those fragments from becoming a confident explanation before the manoeuvre force has completed the vulnerable part of its movement.

The duration of the window depends on the mission. A river crossing may require an hour of reduced enemy understanding. A reserve movement might need twenty minutes. A helicopter assault may need only a few minutes at a particular altitude and route. The relevant planning question is therefore not 'Can we blind the enemy?' but 'How long must the enemy be unable to solve this problem?' That is a more limited and achievable requirement.

A hypothetical example illustrates the distinction. Under normal conditions, an enemy sees increased vehicle traffic, confirms the activity with drones, detects communications and identifies engineering equipment near Axis A. It concludes that the main attack will occur there, increases ISR coverage, moves reserves and allocates fires. In a shaped environment, the same enemy sees convincing activity on Axes A, B and C. Drone teams covering the real route have been struck or jammed. A false headquarters produces traffic near B. Engineers visibly prepare a decoy crossing at C. Smoke obscures a short section of A. The enemy is not blind; it is uncertain. If the real force moves before the uncertainty is resolved, the window has worked.

This returns time to manoeuvre theory. The key variable is reconstruction time: how long it takes the defender to recognise that its picture is wrong, restore sensor coverage, obtain new information, decide what the information means and redirect weapons or reserves. A formation that can complete its decisive movement inside that reconstruction time regains tempo. A formation that remains exposed after the picture is rebuilt becomes vulnerable again.

Figure 2. Creating a Window of Opacity: manoeuvre becomes possible when enemy understanding is degraded for long enough to permit rapid concentration and decisive movement.

Windows of opacity can also occur naturally. Weather, darkness, terrain, urban clutter and vegetation may degrade sensors. Commanders should treat these not as inconveniences but as opportunities. The task is to combine natural opacity with deliberate suppression so that a temporary environmental advantage becomes operationally useful.

11. Autonomy and the Limits of Electronic Denial

Electronic warfare is central to contemporary counter-reconnaissance, but it is not a permanent answer. Electronic warfare refers to military action involving the electromagnetic spectrum: the range of frequencies used by radios, radars, satellite links, navigation systems and many sensors. Jamming can deny or degrade those links. Detection can locate emitters. Deception can introduce false signals. The difficulty is that the enemy adapts.

Fibre-optic control is one example. Autonomy is another. DARPA's Collaborative Operations in Denied Environment, or CODE, programme was designed to allow unmanned aircraft to operate with greater resilience when bandwidth was limited or communications were disrupted. The programme explored software that allowed groups of aircraft to maintain mission intent and collaborate rather than requiring continuous human control of every action. [9]

As onboard processing improves, the relationship between communications and mission execution changes. A traditional unmanned system may depend on a remote operator to interpret video and issue commands. A more autonomous system can potentially navigate, classify objects, prioritise routes or continue a pre-authorised mission even after the data link is lost. The exact level of autonomy varies by system, mission and national policy, and human control over the use of force remains an important legal and ethical consideration. The military point is narrower: breaking the communications link may no longer terminate the mission.

Russia's Geran programme illustrates the wider adaptation cycle. CSIS documented rapid changes in navigation, communications, propulsion, payloads and tactics, with battlefield feedback feeding production at a cadence measured in weeks. When Ukrainian jamming improved, satellite-navigation antennas changed. When interceptors became more effective, Russia experimented with faster variants and additional defensive measures. The lesson is that any fixed countermeasure will face a response. [11]

Future suppression must therefore be layered. Electronic attack remains valuable, but forces also need physical interceptors, navigation deception, passive defence, camouflage, decoys, directed energy where practical, attacks on launch and support infrastructure and software that can be updated quickly. The purpose is not to identify one decisive technology. It is to ensure that the enemy has to solve several different problems simultaneously.

12. Geography Changes the Meaning of Transparency

Any theory based only on Ukraine risks becoming a theory of open European terrain rather than a theory of warfare. Geography changes sensor performance, communications, movement, sustainment and the density of observable signatures. A force that learns the correct lessons from Ukraine must therefore distinguish between principles that are broadly transferable and methods that depend heavily on the environment.

Much of Ukraine's battlefield contains open agricultural land, relatively extensive road networks and lines of sight that favour aerial observation. Tree lines, towns and folds in the ground still provide concealment, but large-scale movement often occurs in spaces where drones can obtain useful views. This makes the Ukrainian battlefield a particularly severe test of visual and thermal signature management.

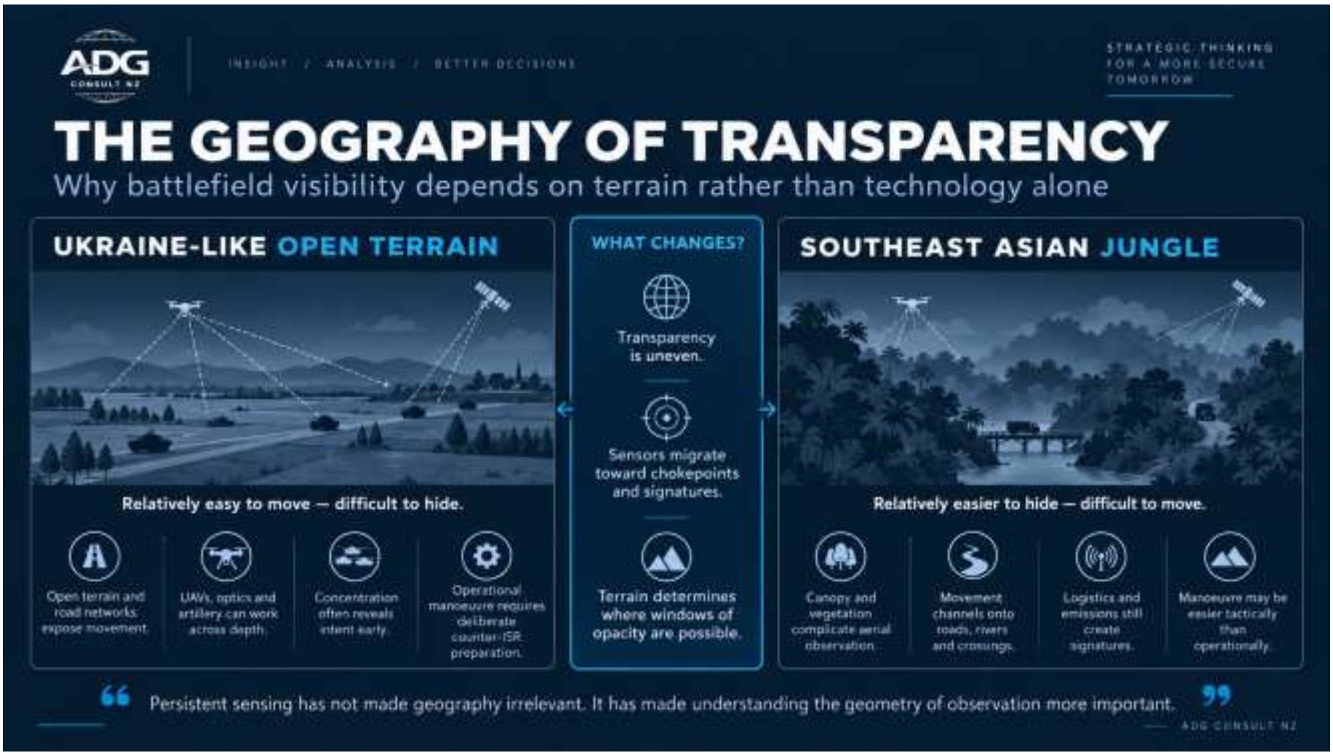

Figure 3. The Geography of Transparency: persistent sensing affects different operating environments differently; terrain shapes both the ability to observe and the ability to manoeuvre.

A tropical jungle reverses part of the problem. U.S. Army and Marine Corps jungle doctrine describes restricted observation, difficult off-road movement, rapid vegetation growth, heavy rainfall, degraded communications and the operational importance of roads, rivers, trails, fords and landing zones. Dense canopy can reduce what an aircraft or optical satellite can see directly at ground level, while vegetation and terrain complicate radio propagation. [10]

This does not make jungle a sanctuary. Radar, signals intelligence, acoustic detection, human reconnaissance and sensors placed on likely routes can still reveal activity. Synthetic-aperture radar, usually called SAR, is a form of radar imaging that can operate through cloud and darkness and can provide information that ordinary optical cameras cannot. Some radar frequencies can also detect features through vegetation better than visible light, although foliage, geometry and target type still impose limitations. The result is not invisibility but a different balance among sensors.

The more important effect may be that movement becomes concentrated. A platoon can move under canopy in ways difficult to observe from above. A brigade cannot sustain itself without fuel, ammunition, vehicles, communications and medical support. Roads and waterways therefore become information chokepoints. Sensors that are less useful across the entire jungle may become extremely useful at bridges, river crossings, ports, airfields, clearings and road junctions. Transparency becomes localised around the points where logistics and mobility are forced into the open.

13. The Jungle Test: Concealment Returns, Mobility Does Not

Southeast Asia provides a useful test of the argument because it exposes a central paradox. The jungle can give manoeuvre back some concealment while simultaneously taking away much of its mobility. This means the conditions for tactical manoeuvre may improve while the conditions for large-scale operational manoeuvre remain demanding.

At small-unit level, dense vegetation can shorten lines of sight, reduce the effectiveness of some aerial observation and allow infiltration close to an opponent. The same vegetation can make navigation difficult, slow movement, restrict vehicle access and complicate command and control. Engagements may occur at short range with little warning. A force trained only for an open, drone-dense environment could therefore overestimate how much warning technology will provide.

At larger scale, sustainment becomes the limiting factor. Fuel tankers do not move easily through primary jungle. Heavy engineering equipment requires routes. Ammunition must be transferred through distribution points. Helicopters need landing zones or hover points. Boats and barges use rivers that can be monitored. Ports and beaches become critical. The more an army attempts to generate operational tempo, the more it must interact with these constrained nodes.

This produces a different counter-ISR strategy. In Ukraine, the priority may be defeating persistent aerial observation across broad sectors. In jungle, the priority may shift toward protecting routes, controlling emissions, securing bridges and crossings, hiding logistics patterns and preventing the opponent from placing unattended sensors along predictable avenues. The reconnaissance battle becomes concentrated around transition points between opaque terrain and exposed infrastructure.

The lesson is that sensor advantage is never independent of geography. A force should not ask whether drones work in jungle as if the answer were binary. It should ask what each sensor can observe, from where, under which weather and canopy conditions, and which unavoidable activities remain detectable. Manoeuvre planning then exploits the gaps while protecting the nodes that cannot be hidden.

14. The Battlefield as a Mosaic of Transparency and Opacity

A more useful model for future warfare is the battlefield as a mosaic. Different parts of the same theatre can possess radically different levels of observability at the same time. The pattern changes with weather, time of day, terrain, electronic-warfare coverage, orbital geometry, sensor availability and the enemy's allocation of attention.

A coastline may be continuously monitored by radar, aircraft, satellites and maritime sensors. Jungle five kilometres inland may be difficult to observe directly. A road leaving the jungle may become highly exposed. An urban area may produce so much visual, thermal and electronic clutter that individual units are difficult to distinguish, while bridges, motorway junctions and open squares become obvious surveillance points. A mountain range may block radio and optical line of sight yet funnel movement through a handful of passes.

This mosaic should be incorporated into terrain analysis. Traditional terrain analysis examines observation, cover, concealment, obstacles, key terrain and avenues of approach. Modern planners need to add sensor geometry. Where can the enemy's cameras see? Where does terrain mask radar? Which areas allow reliable data links? Where are satellite observations most likely to matter? Which roads create unavoidable thermal and dust signatures? Where can smoke or obscurants break visual tracking? Where do civilian emissions create useful background clutter, and where would a single tactical radio stand out?

The result is not a new digital layer separate from geography. Sensor terrain is part of geography. Commanders who understand it can route forces through areas where the enemy's understanding is weaker, time movement for periods when sensing is degraded and place deception where it will be most credible. The same principles that once made dead ground and reverse slopes valuable now apply to gaps in radar, data links and drone coverage.

15. From Hiding Forces to Hiding Intent

Camouflage remains essential, but camouflage by itself seeks primarily to avoid detection. A densely observed battlefield may make that objective increasingly difficult for large formations. The alternative is to conceal intent even when some activity is visible.

This changes the purpose of deception. A convincing deception operation does not merely create a fake object. It creates a plausible story. If the enemy expects a mechanised attack, a false axis may need vehicle movement, engineering work, communications traffic, logistics activity and reconnaissance consistent with an actual offensive. If the enemy possesses several sensor types, the deception must survive cross-checking among them.

This is what multispectral deception means in practical terms. A decoy that looks correct to a daylight camera but has no heat may fail against thermal imagery. A false headquarters that produces radio traffic but no vehicle movement may appear implausible. A fake missile launcher that has the right shape but no radar, communications or maintenance pattern may be identified as a decoy. Future deception therefore requires coordination among visual camouflage, heat generation, electronic emissions, movement and behaviour.

The burden is considerable, but the opportunity grows with the enemy's dependence on automated fusion. A network designed to combine many observations quickly can become highly confident when several sources appear to corroborate one another. If those sources are deliberately manipulated, the speed and efficiency of the network can propagate the wrong conclusion just as efficiently as the right one.

The objective is not to make the enemy believe something absurd. The best deception offers a plausible explanation that fits what the enemy already expects. It forces the opponent to allocate sensors, fires and reserves to protect against a threat that is credible but not decisive. The real manoeuvre then exploits the resources that have been drawn away.

16. Making the Battlefield Lie

The phrase making the battlefield lie describes a condition in which individual observations may be accurate while the overall explanation is false. A drone really does see a launcher. A satellite really does see support vehicles. Signals intelligence really does detect communications. The deception succeeds because the launcher is a decoy, the vehicles are unmanned or expendable and the communications are deliberate false traffic. The sensors are not necessarily defeated. Their interpretation is.

This is more demanding than simple camouflage but potentially more scalable than attempting to destroy every sensor. Commercial satellites cannot easily be eliminated without major escalation. Cheap drones can be replaced. Autonomous systems may continue after communications are interrupted. The defender therefore requires methods that remain useful even when observation persists.

Deception can also create cost imposition. Every reconnaissance sortie directed at a false target is collection capacity unavailable elsewhere. Every expensive missile fired at a decoy is an exchange the defender may welcome. Every reserve moved toward a false threat creates a weakness somewhere else. The important effect is misallocation. Manoeuvre warfare has always tried to create inappropriate enemy dispositions; modern deception can do so through the information system before the physical attack begins.

There is a defensive danger in this logic. Forces that accelerate their sensor-to-shooter process can become highly efficient at acting on incorrect information. Artificial intelligence and automated target recognition may reduce the time required to sort large volumes of data, but machine confidence is not the same as truth. The faster a military acts, the more important it becomes to preserve mechanisms for confirmation, anomaly detection and challenge. Speed without epistemic resilience - the ability to recognise that one's understanding may be wrong - can make a sophisticated force easier to deceive.

The contest therefore moves beyond seeing first. The decisive advantage may belong to the force that can see enough, hide what matters, falsify what cannot be hidden and force the opponent to spend scarce attention on the wrong problem.

17. How Armies Get Manoeuvre Back

If manoeuvre is to return at operationally significant scale, armies need to change the way they sequence combat. A simplified traditional sequence might place concentration before breach and exploitation. In a densely observed environment, concentration may have to occur much later. Forces remain distributed while reconnaissance and counter-reconnaissance shape the decisive area. They create false indicators, degrade selected sensors and isolate the target system. Only when the local information environment is favourable do they aggregate the combat power required for the decisive action.

The resulting sequence is better understood as dispersion, survey, deception, suppression, rapid concentration, manoeuvre, exploitation and renewed dispersion. These are not rigid phases. Several occur simultaneously and repeat. The important point is that information preparation becomes integral to physical movement. The force does not wait until it is moving to worry about whether it is being observed.

Counter-ISR must therefore be represented in command relationships and force design. A manoeuvre commander needs access to electronic warfare, air defence, fires, cyber support where appropriate, deception capability and intelligence analysis that can identify how the enemy's reconnaissance network actually functions. These capabilities cannot operate as separate technical communities. Their effect has to be synchronised around a movement window measured in minutes or hours.

Signature management also has to become ordinary fieldcraft. Every echelon needs to understand how visual, thermal and electronic behaviour reveals it. Radio discipline must be treated as survivability. Logistics units need deception and dispersion methods. Headquarters need the ability to operate with intermittent connectivity and smaller physical footprints. Artillery and air defence require displacement routines that assume they are being watched. A formation that regards these measures as specialist activities will reveal itself before the specialists can protect it.

Rapid concentration becomes a core capability. If forces must remain dispersed for survivability, they need command systems, mobility, rehearsals and logistics that allow them to generate local mass quickly. This may involve concentrating effects before platforms: long-range fires, unmanned systems and electronic attack can shape a sector while physical formations remain distributed. Physical concentration then occurs for the shortest time required to create a decision, after which the formation disperses again.

The most useful planning metric may be reconstruction time. Commanders should ask how long the enemy needs to restore a coherent picture after its reconnaissance architecture is degraded. If the answer is thirty minutes, the force must complete the vulnerable movement inside that period or extend the disruption. This converts counter-reconnaissance from an abstract ambition into a measurable operational requirement.

18. Force Design, Training and Procurement for the Return of Manoeuvre

The force-design implications are wider than buying more drones. Western militaries require a portfolio that combines exquisite systems with cheap, numerous and replaceable ones. High-end sensors and platforms remain necessary for range, survivability, payload and quality that inexpensive systems cannot match. Attritable systems provide mass, persistence and the ability to accept risk. The same portfolio principle should apply to counter-reconnaissance.

Air defence and counter-UAS forces need economically sustainable layers. A formation cannot use a million-dollar interceptor for every cheap quadcopter and expect to remain viable through a long campaign. Passive detection, machine-assisted cueing, low-cost interceptor drones, guns, electronic warfare, directed energy where mature enough, obscurants and physical protection all have roles. The appropriate mix varies by target value and threat.

Deception requires institutional investment rather than improvisation. Units need decoys, emitters, thermal simulators, signature-replication equipment and personnel trained to build realistic false patterns. Exercises should allow opposing forces to use commercial satellite imagery, signals collection and drones so that deception can be tested against a real collection problem. A false target that survives inspection by friendly planners but fails immediately against an adversary sensor is not a useful capability.

Procurement speed is equally important. CSIS's analysis of the Geran programme shows a weapons-development cycle in which field experiments are tested, successful modifications are scaled and unsuccessful ones are discarded on a timescale measured in weeks. Western acquisition systems designed around long requirements cycles and highly controlled configuration changes can struggle to match this tempo. The implication is not that safety, reliability and accountability should be abandoned. It is that wartime systems need pathways for rapid software, sensor and component changes without restarting the entire acquisition process. [11]

Training needs to recreate the psychological effect of observation. Soldiers behave differently when they know any stationary vehicle may be detected, any radio transmission may be located and any large gathering may be targeted. Exercises that allow headquarters to operate continuously from comfortable command posts with uninterrupted communications teach the wrong habits. A force will not learn to disperse, deceive and operate under uncertainty unless the exercise rewards those behaviours and punishes signatures.

Professional military education must also reconnect technology with geography. Officers should understand enough about radar, thermal imaging, satellite collection, data links and electronic warfare to reason about what the enemy can see in a particular environment. They do not need to become engineers. They need to be able to ask the correct operational questions and integrate technical advice into manoeuvre planning.

19. Tactical Manoeuvre Is Not Operational Manoeuvre

A further distinction is necessary because small-unit movement can return before operational manoeuvre does. Tactical manoeuvre concerns movement and advantage at the level of individual engagements and local formations. Operational manoeuvre concerns the ability to move, concentrate and sustain forces on a scale large enough to alter the structure of a campaign. The two are connected, but success at one level does not automatically produce success at the other.

A squad or platoon can exploit dead ground, vegetation, darkness or a temporary gap in drone coverage. A company may infiltrate through a weakly observed area and achieve local surprise. These actions matter, but they do not solve the problem of moving artillery, air defence, engineers, fuel, ammunition, casualty evacuation and reserves behind the assault. Operational manoeuvre fails if the leading element advances while the system required to sustain it remains exposed and unable to follow.

Ukraine illustrates this difference clearly. Local penetrations and limited mechanised attacks continue to occur, yet converting them into sustained operational breakthroughs remains difficult. The obstacle is not simply the forward defensive line. It is the ability of both sides to observe reinforcement routes, strike logistics and move reserves into threatened sectors before a penetration becomes a collapse. The same reconnaissance-strike architecture that constrains the initial attack also constrains exploitation after success. [1][14]

This means the return of manoeuvre should not be measured only by whether armoured vehicles can cross the first several kilometres. The more demanding test is whether the attacker can maintain tempo beyond the initial breach. Can bridging and engineering assets survive? Can fuel reach the advancing force? Can air defence displace with it? Can command posts remain connected without becoming fixed targets? Can reserves follow without revealing the axis? If the answer is no, tactical movement may be possible while operational manoeuvre remains suppressed.

The concept of windows of opacity therefore has to extend in depth. It is not enough to create uncertainty at the point of contact. A successful operation may require a series of overlapping windows across routes, logistics nodes, crossing points and command locations. The attack must move from one locally favourable information condition to the next faster than the defender can reconstruct the whole pattern. In this sense, operational manoeuvre becomes a problem of chaining temporary information advantages together.

Geography again matters. Dense jungle may make the leading infantry harder to observe while making the sustainment network more predictable because it must use a limited number of roads and waterways. Desert may make both assault and logistics highly visible. Urban terrain can conceal small formations yet expose bridges and intersections. The scale at which manoeuvre returns will therefore depend not only on whether combat troops can hide, but on whether the entire operational system can move without presenting the enemy with a coherent and targetable pattern.

20. Command and Control Inside the Window

Creating a window of opacity is of limited value if the force cannot command and coordinate itself while operating inside it. This creates a tension at the centre of modern manoeuvre. The attacking force wants to reduce its own electronic signature and deny the enemy access to communications, but it also needs enough connectivity to coordinate fires, movement, air defence, logistics and rapidly changing tactical decisions.

The solution is unlikely to be permanent high-bandwidth connectivity. U.S. Army analysis from Ukraine emphasises the vulnerability of communications equipment and the need for signature discipline, distribution and the ability to operate when networks are degraded. The implication is that command systems must tolerate interruption rather than treating uninterrupted connectivity as a normal condition. [4]

Mission command becomes particularly important in this environment. Mission command is the practice of giving subordinate leaders a clear purpose, desired outcome and appropriate freedom to act when detailed instructions are unavailable or conditions change. A formation that requires constant permission from a distant headquarters may be unable to exploit a short information window because the communications needed to coordinate every decision reveal the force or consume too much time. A formation whose subordinate commanders understand the intent can continue moving when links are intermittent.

This does not mean abandoning networks. It means using them more intelligently. Communications can be burst rather than continuous, transmitted from displaced relays, routed through multiple paths and prioritised according to operational importance. Some information can be processed locally rather than sent to a central headquarters. Command posts can be smaller and distributed. The force can plan periods of deliberate electronic silence during the most exposed movement and reconnect when the tactical situation allows.

The enemy will attempt to impose the opposite condition. Russia's efforts to jam Starlink-supported Ukrainian drone operations in 2026 demonstrate that even relatively resilient commercial communications can become contested. Ukrainian forces have responded by locating and attacking some of the jamming systems and by adapting networks and operating procedures. The episode reinforces a wider principle: communications advantage is temporary and must be actively defended. [12]

Command and control therefore becomes part of the manoeuvre bargain. The force has to retain enough information flow to preserve cohesion while emitting little enough to avoid rebuilding the enemy's picture. This is not purely a technical optimisation. It demands rehearsed procedures, disciplined staffs and subordinate leaders capable of operating with incomplete information. A technologically sophisticated formation that becomes paralysed when connectivity is degraded may be less manoeuvrable than a simpler force whose commanders can continue acting on intent.

The operational opportunity created by decision denial is ultimately perishable. Command systems must be designed around that perishability. Information should move quickly enough to exploit the window but not so extravagantly that the communications architecture itself reveals the operation. In practical terms, the army that gets manoeuvre back will need to be both highly networked and capable of temporarily behaving as though the network is not guaranteed.

21. Measuring the Window: When Is It Favourable Enough to Move?

The concepts of decision denial and windows of opacity are useful only if commanders can recognise when the desired condition actually exists. There is unlikely to be a universal threshold at which a battlefield suddenly changes from transparent to opaque. The required condition is mission-specific. A company moving five kilometres through broken terrain may need only a short interruption in local drone coverage. A brigade crossing a river or attempting operational exploitation needs a much deeper and more durable advantage because its engineers, logistics, air defence, command posts and reserves must all survive the movement. The relevant question is therefore not whether the enemy has been blinded, but whether its remaining reconnaissance system is still capable of solving the particular problem the manoeuvring force is about to present.

One of the most useful measures is latency: the time between detection and effective response. If an enemy normally detects movement, confirms it and generates fires within several minutes, then merely reducing the number of sensors may achieve little. If suppression, deception and communications disruption extend that process long enough for the force to pass through the exposed area, the same enemy network may remain technically functional while becoming operationally inadequate. RUSI's work on Ukraine is important here because it shows that successful formations are not seeking abstract information dominance; they are degrading the reconnaissance and supporting systems that matter to a specific assault and exploiting the resulting period before the defender can recover. [1]

Reconstruction time is the complementary measure. Reconstruction time is the period the adversary requires to restore a coherent picture after its sensor network has been disrupted or deceived. It includes replacing or repositioning sensors, restoring communications, separating genuine indicators from false ones, reallocating attention and deciding how to respond. A manoeuvring force that requires forty minutes to cross an exposed corridor does not need permanent information superiority if the defender requires an hour to reconstruct what is happening. Conversely, a ten-minute disruption is of little value if the force needs two hours to move its critical equipment. The relationship between movement time and reconstruction time should therefore become an explicit planning consideration.

Coverage continuity matters more than the number of hostile sensors destroyed. A formation may shoot down several drones and still achieve nothing if another system continues watching the only bridge, road junction or breach lane that matters. Counter-reconnaissance planning should therefore map functions and coverage rather than simply count platforms. The commander needs to know which sensor provides the decisive view, which alternative system can replace it, which communications link passes the information onward and where the next layer of observation begins. The objective is to create a gap in the enemy's ability to understand the route or action that matters, not to generate an impressive tally of destroyed unmanned aircraft.

Confidence is harder to measure but equally important. An adversary may continue observing the battlefield while becoming progressively less certain about what those observations mean. Deception is successful when it forces the enemy to retain several plausible explanations for the same activity, delay commitment or allocate resources against a false problem. The attacking force will rarely know exactly what the opposing commander believes, so this condition has to be inferred from behaviour: changes in sensor allocation, reserve movement, fires, air-defence posture, electronic activity and the enemy's reaction to decoys can all provide clues. The purpose is not to assume deception has worked because the plan was clever. It is to look for evidence that the opponent's decisions are actually being affected.

The window also has a friendly side. A force can suppress hostile communications so aggressively that it interferes with its own command, navigation or unmanned systems. It can generate smoke that hides the crossing from the enemy while also obscuring friendly observation. It can disperse so widely for survivability that concentration takes longer than the information advantage lasts. A useful window of opacity therefore exists only when the attacking force retains sufficient command, navigation, reconnaissance, air defence and logistical coherence to exploit it. The desired condition is not mutual blindness. It is asymmetry: the enemy understands less, more slowly or less reliably than the force attempting to manoeuvre.

This has direct implications for training. Exercises intended to prepare formations for manoeuvre against a capable opponent should instrument the reconnaissance battle as seriously as the physical one. Opposing forces need realistic drones, electronic sensing, data links, commercial-imagery injects, deception targets and strike processes. The exercise should record how long it takes to detect a movement, how long confirmation takes, when the target becomes actionable, how long a disrupted sensor network takes to recover and whether false indicators cause genuine misallocation. U.S. Army analysis of communications survivability in Ukraine reinforces why this matters: emitting, remaining stationary or following predictable patterns can expose a formation quickly, and forces that train with continuous connectivity and permissive observation conditions risk learning habits that will fail in combat. [4]

Ultimately, the decision to move remains a command judgement rather than a technical certification. There will rarely be a moment when every indicator turns favourable. The commander must decide whether the enemy's current uncertainty is sufficient for the mission, whether the force can complete the most vulnerable movement before the picture is rebuilt and whether the advantage justifies the residual risk. In this sense, armies do not get manoeuvre back by discovering a permanent technological answer. They get it back by becoming able to recognise, create and exploit temporary periods when the enemy's reconnaissance-strike system is performing below the level required to stop them.

22. The Limits of the Argument

There is a risk that the concept of windows of opacity becomes another technological shortcut. It is not. Degrading reconnaissance does not remove minefields, artillery, prepared defences, difficult terrain or determined infantry. A force that creates a local information advantage still has to breach obstacles, sustain itself, protect its flanks and defeat the enemy physically.

There is also no reason to assume that the defender will remain passive. The same technologies that allow an attacker to deceive and suppress can be used defensively. Autonomous sensors can be distributed in depth.

Commercial satellite providers can increase observation. AI-assisted processing can reduce the time required to search data. Fibre-optic links can bypass jamming. Radar can supplement optical imagery. The competition will remain dynamic.

Nor should the paper imply that every battlefield will become equally hostile to manoeuvre. Geography, force quality, air superiority, civilian density, weather, infrastructure and the availability of sensors all matter. A technologically sophisticated force fighting an opponent with weak ISR may retain substantial freedom of movement. A low-technology force in dense jungle may achieve surprise against a more advanced opponent by exploiting terrain. The relevant question is always relational: what can this enemy observe and act upon, in this environment, at this time?

The argument is therefore deliberately bounded. Persistent sensing has made large-scale movement harder and has reduced the value of early concentration. Manoeuvre remains possible when forces can degrade, delay or deceive the systems that convert observation into action. The result is an operational opportunity, not an automatic breakthrough.

23. Conclusion: The Price of Admission

The contemporary battlefield is more observable than any before it. Small drones have pushed aerial reconnaissance to low tactical echelons. Commercial space has increased access to repeated overhead imagery. Electronic sensing reveals emissions. Digital networks move information quickly. Precision weapons allow observations to generate effects across greater depth. These developments have made concentration, sustainment and movement increasingly dangerous when the enemy's reconnaissance-strike system is allowed to operate uninterrupted.

The response should not be to declare manoeuvre warfare dead. Manoeuvre warfare is a theory of creating advantage through surprise, tempo, dislocation and the concentration of strength against weakness. None of those ideas depends on a permanently opaque battlefield. They depend on the opponent failing to solve the situation before the manoeuvring force exploits it.

Future forces must therefore fight for control of perception. They need to understand the enemy's sensor architecture, destroy what must be destroyed, jam what can be jammed, deceive what cannot be removed, exploit terrain and weather, and move before the adversary reconstructs the truth. Counter-reconnaissance becomes a manoeuvre function. Deception becomes a routine component of combat. Signature management becomes fieldcraft. Reconstruction time becomes an operational measure.

Geography prevents any single technological conclusion from becoming universal. Ukraine demonstrates the extreme difficulty of movement across a densely observed open battlefield. Jungle demonstrates that concealment can return while mobility and logistics become more constrained. Cities, mountains, deserts, littorals and archipelagos each create their own pattern. The future battlespace is therefore best understood as a changing mosaic of transparency and opacity.

The army that learns to manipulate that mosaic can regain freedom of action. It does not need to make itself invisible everywhere. It needs to create uncertainty at the decisive place, preserve that uncertainty long enough to concentrate and move, then exploit faster than the opponent can rebuild an accurate picture. The purpose is not to blind the enemy forever. It is to make the enemy late, uncertain or wrong at the moment that matters.

This changes what successful suppression should look like. A commander should not be satisfied merely because a large number of drones have been destroyed or because an electronic-warfare system has generated an impressive area of interference. Those are activities, not outcomes. The operational outcome is a measurable reduction in the enemy's ability to understand the decisive action in time to stop it. A single surviving sensor over the critical crossing can matter more than ten destroyed systems elsewhere. Equally, an enemy may retain many functioning sensors yet still be unable to decide because deception, latency and conflicting reports have made its picture unreliable. The standard is therefore whether the reconnaissance-strike system can still solve the commander's problem, not whether every component has been eliminated.

The same logic suggests that armies should think about the relationship between movement time and reconstruction time in much the same way they already think about range, endurance and time on target. If the vulnerable portion of a manoeuvre requires thirty minutes, the information advantage must last at least long enough for that movement and the essential supporting system to pass through it. If the defender can rebuild its picture in ten minutes, the window is too short unless the attacker can renew the disruption. At operational scale, manoeuvre may therefore depend on a chain of overlapping windows rather than a single moment of blindness: one for the breach, another for the logistics route, another for the reserve movement and another for exploitation. The force that can repeatedly create such asymmetries can restore tempo even on a heavily observed battlefield.

This is also why the A2/AD problem should be viewed more broadly. A defensive system that makes an area lethal to crewed aircraft, ships or ground formations remains strategically important, but it is incomplete if the adversary can still obtain reliable information from satellites, attritable unmanned systems, electronic collection or unattended sensors and then generate effects from outside the denied area. Physical denial and information denial are increasingly separable. The stronger form of denial is therefore decision denial: preventing the adversary from converting whatever it can still observe into timely and trustworthy action. The contest is no longer only over who can enter a space. It is over who can correctly understand that space while the other side is trying to manipulate the picture.

Geography ensures that this contest will never have a single technological answer. An army designed only around the experience of open Ukrainian farmland may be badly prepared for jungle, dense urban terrain, mountains or an archipelago. In jungle, the problem may move away from continuous overhead observation and toward roads, rivers, emissions, crossings and sustainment nodes. In a city, clutter can hide small forces while bridges, intersections and major logistics movements remain conspicuous. The underlying principle remains the same: identify where the enemy's understanding is strongest, where it naturally weakens and which portions of that information architecture must be disrupted or deceived to create freedom of action. Terrain still matters; modern sensing adds another layer to terrain rather than abolishing it.

The institutional implication may be as important as the technological one. Forces that expect to regain manoeuvre cannot treat counter-reconnaissance, electronic warfare, deception and signature management as specialist services applied after the manoeuvre plan has already been written. They have to become part of the manoeuvre plan itself. Commanders need to understand enough about sensor coverage, data links, commercial imagery and electronic signatures to ask the right operational questions. Subordinate formations need mission command and communications discipline so they can continue when networks are degraded. Procurement systems need equipment and software that can be adapted at the pace of the threat. Exercises need an opposing force capable of observing and targeting realistically, otherwise formations will rehearse manoeuvre in an information environment they are unlikely to receive in war.

None of this restores a romantic form of free movement in which large formations simply disappear and reappear at will. The future battlefield will remain dangerous, information-rich and contested. Minefields, artillery, logistics, air defence, force protection and basic combined-arms competence remain decisive. The argument is narrower and more practical: persistent observation does not make manoeuvre impossible if the observation can be degraded, delayed, confused or deprived of meaning for long enough. The army that can manufacture those conditions gains opportunities that the army accepting transparency as fixed terrain does not.

This is the route by which armies get manoeuvre back. The price of admission is the ability to contest observation itself and, where observation cannot be prevented, to contest its meaning. **The battlefield of the future may be impossible to hide - but it may still be possible to make it lie.**

Source Notes and References

This Insight Paper is an open-source strategic assessment. The concepts of decision denial, windows of opacity and Suppression of Enemy Reconnaissance are used here as analytical frameworks developed for this paper; they should not be read as claims that those exact terms constitute current NATO or U.S. doctrine. Contemporary battlefield claims remain subject to wartime deception, incomplete public reporting and rapid technical change. Sources below are selected for the specific factual or doctrinal claims cited in the text. Assessment cut-off: 9 September 2026.

[1] Jack Watling, 'Emergent Approaches to Combined Arms Manoeuvre in Ukraine,' Royal United Services Institute, 23 October 2025. https://www.rusi.org/explore-our-research/publications/insights-papers/emergent-approaches-combined-arms-manoeuvre-ukraine

[2] U.S. Department of Defense, 'The Future Character of War,' keynote address by Deputy Secretary of Defense Kathleen H. Hicks, December 2024. https://www.defense.gov/News/Speeches/Speech/Article/3992669/the-future-character-of-war-keynote-address-by-deputy-secretary-of-defense-kath/

[3] Center for Strategic and International Studies, 'Russia's Cap on Partner Aid: Institutional Rigidity and the Limits of External Support,' August 2026, including the case of commercial satellite imagery supporting the 4 June 2026 strike on Shahed-launch infrastructure at occupied Donetsk Airport. https://www.csis.org/analysis/russias-cap-partner-aid-institutional-rigidity-and-limits-external-support

[4] U.S. Army, 'Tactical Communication Survivability in the Hyper-Lethal Battlespace,' 31 July 2026. https://www.army.mil/article/294285/tactical_communication_survivability_in_the_hyper_lethal_battlespace

[5] U.S. Department of Defense, Deputy Secretary Kathleen Hicks, 'The Urgency to Innovate,' 28 August 2023, on Replicator and all-domain attritable autonomous systems. https://www.defense.gov/News/Speeches/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/

[6] Reuters, 'Iran says it captured US submarine drone in Strait of Hormuz,' 8 September 2026. https://www.reuters.com/world/middle-east/iran-says-it-captured-us-submarine-drone-strait-hormuz-2026-09-08/

[7] Reuters, 'From steppe to sea, a Ukrainian drone unit hunts Russian ships,' 24 July 2026. https://www.reuters.com/world/europe/steppe-sea-ukrainian-drone-unit-hunts-russian-ships-2026-07-24/

[8] Reuters, 'Russia evades Ukraine electrical substation defences with small, unjammable drones,' 10 July 2026. https://www.reuters.com/business/aerospace-defense/russia-evades-ukraine-electrical-substation-defences-with-small-unjammable-2026-07-10/

[9] Defense Advanced Research Projects Agency, 'Collaborative Operations in Denied Environment (CODE).' https://www.darpa.mil/research/programs/collaborative-operations-in-denied-environment

[10] U.S. Army / U.S. Marine Corps, ATP 3-90.98 / MCTP 12-10C, 'Jungle Operations,' 24 September 2020. https://www.marines.mil/Portals/1/Publications/MCTP%2012-10C.pdf

[11] Kateryna Bondar and Nicole Errera, 'From Shahed to Geran: How Russia Continues to Reinvent the One-Way Attack Drone,' Center for Strategic and International Studies, 4 September 2026. https://www.csis.org/analysis/shahed-geran-how-russia-continues-reinvent-one-way-attack-drone

[12] Reuters, 'Russia tries to jam Musk's Starlink systems to counter Ukrainian drones,' 8 July 2026. https://www.reuters.com/business/aerospace-defense/russia-tries-jam-musks-starlink-systems-counter-ukrainian-drones-2026-07-08/

[13] Marcus Welsch et al., 'The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine,' Center for Strategic and International Studies, 7 July 2026. https://www.csis.org/analysis/geography-coercion-russian-missile-and-drone-campaigns-ukraine

[14] Reuters, 'Russian drive on Donetsk region puts Kyiv's new commanders to the test,' 8 September 2026. https://www.reuters.com/world/europe/russian-drive-donetsk-region-puts-kyivs-new-commanders-test-2026-09-08/