

I'm not robot



NATO Seeks to Enhance Multimodal Operations for Stronger Deterrence and Defense Capabilities Nations on both sides of the Atlantic have finally recognized the need for a strengthened defense-industrial base after decades of neglect. However, this newfound awareness is being overshadowed by an increasingly complex threat landscape that poses significant challenges to transatlantic security and defense. Allies along NATO's eastern borders are facing off against a Russian adversary that shows no signs of backing down, despite its depleted land forces. Russia's air, strategic, and naval capabilities remain largely intact, and it could potentially reconstitute its land-based warfighting abilities within a few years. The Alliance must also contend with challenges emanating from beyond its borders, including China's coercive behavior, cyber threats, and regional instability in NATO's southern neighborhood. In this era of uncertainty, maintaining a warfighting advantage will depend on NATO's continued modernization and ability to operate across multiple domains at speed and scale. To address these challenges, the report recommends targeted investments in capabilities such as sensor-shooter networks, artificial intelligence-enabled agile logistics, and other approaches that can be implemented quickly without massive budget outlays or long acquisition processes. The goal is to accelerate NATO's transformation into a multidomain warfighting machine, with a focus on practical and attainable solutions that can be pursued by countries of all sizes. A framework for thinking about platforms that can complement existing US initiatives and contribute meaningfully to interallied efforts is also presented in the report. While it leaves out more expensive and complex capabilities that are currently dominating NATO's Defense Planning Process, it provides a starting point for discussions on how to prioritize investments and achieve meaningful impact in the near term. The development of a NATO-wide integrated air- and missile-defense system is crucial for the alliance's future security. Despite its absence in the war in Ukraine, such capabilities would have proven useful in countering Russian air dominance. Russia's lack of assured command-and-control systems led to the collapse of its initial offensive and resulted in the deaths of dozens of officers. NATO nations are already pursuing these capabilities and must continue to invest in their ability to execute military operations across domains today. This report provides a concrete path forward for NATO, recommending selective priorities for MDO initiatives that can be accomplished in the near to medium term with significant effects on allied force posture. The value of establishing a near- and medium-term MDO construct lies in its ability to enhance sensing, command and control, and kinetic and nonkinetic fires, ultimately undergirding survivability. NATO's Multi-Domain Operations Concept Aims to Outpace Adversaries The North Atlantic Treaty Organization (NATO) is shifting its focus towards multi-domain operations (MDO), which requires the alliance and its member countries to work at a faster pace across all five operational domains. This concept, developed by NATO's Strategic Commands, aims to synchronize military activities with non-military efforts to create converging effects in various environments. Multimodal operations are being explored by NATO member states in various ways, with Canada favoring pan-domain operations and the US having its joint warfighting concept (JWC). While there is no official definition of multimodal operations within NATO, some countries have started developing conceptual frameworks for integration. The French Armed Forces participated in the Orion exercise, a multiphase drill testing capabilities in response to a scenario simulating multimodal conflict. Canada has also embarked on an Agile Pan-Domain Command and Control Experimentation Endeavour (APCCXe) using data analytics and AI-enabled tools. Smaller member states, such as Portugal, have participated in exercises like Real Thaw 2023 to test interoperability and combined operations. However, the majority of member states are still behind the US in developing multimodal readiness. The US joint force is navigating an increasingly interconnected operational environment, requiring a new paradigm for future warfare. Gen. Mark A. Milley describes this shift as a "strategic inflection point" that will redefine the character of war. The concept of Joint All-Domain Command and Control (JADC2) aims to create a networked "kill web" connecting sensors and fires across domains, enhancing the US military's ability to prevail in high-stakes conflicts. While other allies are exploring similar approaches, the US is ahead in operationalizing this concept, integrating Multi-Domain Operations (MDO) capabilities at the operational and tactical levels. The Defense Department's CJADC2 strategy empowers Joint Force Commanders with the tools needed to command across all warfighting domains. To implement JWC, each military service is developing initiatives to build joint force capacity for combined and joint operations across domains. The US Army, in particular, is taking a comprehensive approach to MDO through its Field Manual No. 3-0. Key initiatives include the establishment of Multi-Domain Task Forces (MDTFs), which will synchronize long-range precision effects with long-range precision fires. Other notable efforts include the Air Force's Advanced Battlefield Management System (ABMS), which seeks to create an Internet of Things that uses AI to integrate data and accelerate decision-making in the battlespace. The US Air Force is reorganizing its structures to integrate into the Department of Defense's joint all-domain command and control endeavor, called JADC2. The new structure, called the DAF Battle Network, aims to facilitate service integration. The Navy has also been working on a project called Project Overmatch, which enhances software capabilities for connectivity among systems. In contrast, the Army is focusing on building sensor-shooter networks enabled with AI capabilities through Project Convergence. Meanwhile, the Marine Corps has released A Concept for Stand-In Forces as part of its Force Design 2030 strategy, prioritizing agility, efficiency, and technological advancement to meet future challenges. The concept of stand-in forces (SIF) aims to enhance situational awareness, complete kill webs, and disrupt potential adversaries by providing a joint force solution. SIF can be composed of personnel from various services and allies, fostering interallied cooperation and a joint effort. In the context of NATO's military operations, effective integration of member approaches is crucial to complement comparative advantages. NATO's ability to execute military operations relies on its members working together to integrate their national approaches to Military Decision-Making Ontology (MDO). Operationalizing MDO and bolstering interallied coordination are key lines of effort for the Alliance. Effective organization and coordination of member states' efforts will enable tactical operations across domains, while a lack of investment in MDO integration may undermine NATO's defense plans. The ongoing Ukraine-Russia war offers valuable lessons for NATO's MDO activities. Ukrainian forces have leveraged shared intelligence with US and European partners, combined with their own intelligence apparatus, to establish an effective targeting capability. This success demonstrates the importance of interlinking technologies, such as sensors, satellites, machine learning, and software, to create dynamic systems that provide actionable results. The innovative use of commercial and military technologies by Ukrainian conscripts has been particularly noteworthy, enabling them to network and interact more efficiently than Russian soldiers. The interlinked system employed by the Ukrainians, supported by NATO allies and open-source companies, has facilitated collection, analysis, and translation of data into informed decision-making processes. The armed forces have created a data-driven command-and-control system using both public and private technologies across four dimensions: collection, connection, analysis, and action. This innovation is crucial to Ukraine's strategic resilience, as highlighted by Audrey Kurth Cronin in her article "Open Source Technology and Public-private Innovation Are the Key to Ukraine's Strategic Resilience" on War on the Rocks (August 25, 2023). A key factor in Ukraine's sensing operations has been its ability to combine military and commercial capabilities. The Delta Situational Awareness Systems, for instance, provide a comprehensive picture of the battle space by collecting data from various sources, including sensors and open and secret sources. This system is user-friendly and can be accessed on digital maps displayed on laptops, tablets, or mobile phones. Ukraine's reliance on communications facilitated by commercial satellite company Starlink has been crucial to its military capabilities. Starlink's network of low-orbit satellites operated by SpaceX provides reliable communication services, even in emergencies. The low orbit of these satellites allows them to broadcast at relatively higher power, making them more resilient against Russian jamming efforts. The Pentagon's reliance on private companies for low-earth orbit-enabled communications in the context of the Ukraine conflict raises concerns about overreliance, as demonstrated by Elon Musk's refusal to provide Starlink support for Ukraine. This highlights the importance of maintaining both military and commercial satellite capabilities while leveraging commercially available LEO capabilities. Additionally, contracts with private companies should ensure that they cannot unilaterally alter their networks in a way that would negatively impact warfighting capabilities. Effective command and control, including coordinated targeting for fires, has been established through the combined use of commercial and military technologies. This includes GIS Arta, a geographic information system based on commercial technology that links targeting information with strike capabilities, and Kropyva, an intelligence mapping and artillery software populated by information from unmanned aerial systems. The war has also demonstrated the benefits of lower-cost unmanned aerial vehicles (UAVs), both for sensing and striking. The widespread use of commercial products, such as DJI's Phantom 3 or AeroVironment's Quantix Recon, has significantly benefited sensing capabilities, with individual military units using these drones to conduct intelligence, surveillance, and reconnaissance missions. By May 2022, Ukraine had fielded 6,000 commercial drones to provide surveillance capabilities to military units, which they later expanded into an "Army of Drones". Ukraine's drone war has been gaining momentum with an estimated 10,000 drones being lost by the Ukrainians every month. This is largely due to low-cost drone capabilities that have been provided by both public and private sources. According to an Economist report, these drones are being used to target fuel depots, logistics, ammunition dumps, and delivery routes, providing valuable intelligence to the military. A recent strike hit a Tu-22m strategic bomber based near Novgorod, according to Detective, a drone coordinator in Ukraine's military intelligence. The drones have been instrumental in helping the Ukrainians respond to appeals from their field brigades, who are aware of the location of Russian arms but lack the capability to target them. Another significant strike capability is provided by "first person view" drones, which are flown by operators wearing goggles that display a video feed from the drone as it flies. These drones are assembled by volunteers or soldiers themselves using components funded by fundraisers, making them extremely cheap to produce. One Ukrainian-made Pegasus attack drone costs just \$462 to buy. Despite their low cost, FPV drones have a relatively low success rate in destroying targets, with operators reporting a 50%-80% failure rate compared to the 90% or more success rate of American javelin anti-tank missiles. Cyber resilience has also been critical to Ukraine's military effort, with a defensive effort that government officials and technology executives describe as unprecedented. The war has inspired a collaborative effort between governments, private companies like Google and Microsoft, Western allies such as the US and Britain, and social media giants like Meta, who are working together against Russia's digital aggression. US Military Leverages Commercial Capabilities to Enhance Operations The US military has been actively utilizing commercial technologies to support its operations, with significant advancements in recent years. Low-Earth Orbit Satellites: The use of low-earth orbit satellites has become more prevalent, shifting the focus from higher-orbit satellites. Companies like Planet, Capella Space, and Maxar are providing critical sensing capabilities, complementing the US military's existing systems. Commercial Launch Capabilities: The Defense Department (DOD) has been utilizing private-sector launch providers, such as SpaceX, to launch satellites into space. This includes reusable rockets for commercial satellites and planned satellite launches with 163 total satellites. Aerial and Maritime Surveillance: The US Central Command has successfully employed low-cost unmanned vehicles based on commercial technology for surveillance operations. AI capabilities have enhanced the effectiveness of these efforts, with notable examples including the deployment of sea drones in the Persian Gulf. Exercise with Regional Navies: The task force has conducted a series of exercises with regional navies to develop and implement the use of unmanned platforms, with the aim of deploying eighty devices by the end of 2023. Simply said, having a close connection with industry can accelerate advancements by several orders of magnitudes. This is according to an Al-Monitor quote from Szuba, "US Top Middle East Commander Tests New Model." The Air Force's Task Force 99 utilizes commercially available drones for air domain awareness, which are linked by a mesh network. As Lt. Gen. Alexis Grynkewich explained, the surveillance capability is enhanced when paired with AI. Task Force 99 was created to combine unmanned and digital technologies to solve problems more efficiently. This initiative aims to fill gaps in various domains. The Replicator initiative has been established by DOD to field attributable autonomous systems at scale. Deputy Secretary Kathleen Hicks described it as creating a new state-of-the-art leveraging less expensive, autonomous systems that can be updated or improved quickly. The goal is to field multiple thousands of these systems within the next 18-24 months in various domains. Implementing these initiatives will significantly enhance NATO's deterrence and defense capabilities. Each initiative can be accomplished within one to five years and is relatively inexpensive. This approach has already been effectively used by Ukraine, as demonstrated by its use of low-cost, unmanned aerial vehicles in the conflict with Russia. DOD's Replicator initiative shows that senior US defense leadership has incorporated this lesson into their thinking. The rationale behind these initiatives is clear: high-end unmanned capabilities are costly, with systems like the US Gray Eagle and Reaper costing millions of dollars per copy. This is why Task Force 99 uses commercially available drones linked by a mesh network to enhance surveillance capability when paired with AI. The initiative aims to fill gaps in various domains using less expensive, autonomous systems that can be updated or improved quickly. Note: I've kept the original text's language and only paraphrased it for better understanding. The US Air Force is considering the development of a "Loyal Wingman" drone, which would enable it to conduct AI-enabled teaming missions alongside F-35s. However, the project's estimated cost range is between \$3 million and \$25 million per unit, with some estimates suggesting that the final price could be as high as \$40 million. In contrast, the Replicator initiative aims to provide similar capabilities at significantly lower costs, potentially as low as \$1 million per unit. The Replicator project's goal is to augment the US Air Force's capabilities with less complex and inexpensive systems, comparable to those being used in Ukraine. This would enable NATO to enhance its Intelligence, Surveillance, and Reconnaissance (ISR) capabilities, add mass to battles, and establish an offense-defense cost ratio in favor of the alliance. The initiative has several focus areas, including maritime surveillance networks for the Baltic, Black, and Mediterranean seas, as well as ground-based capabilities in a ubiquitous sensing and targeting grid is potentially highly effective. The project's success hinges on cooperative efforts between the US and its NATO allies, as well as the development of low-cost hardware and software. If successful, it could provide a significant advantage to the alliance in terms of cost and capability. Utilizing a swarm of unmanned drones equipped with various sensors, the United States and Taiwan could collectively monitor and control hundreds of vessels in the Taiwan Strait. These drones would process data onboard using edge computing and employ automatic target recognition algorithms to identify different types of ships. The system's AI-driven grid would then assign targets to incoming missiles, ensuring precise strikes against enemy vessels. In addition to this concept, NATO could adopt similar strategies for sea control in other critical regions such as the Baltic, Black, and Mediterranean seas. Moreover, leveraging a sensing and targeting grid would enable effective defense against Russian land forces by employing unattended ground sensors. The "Air-Land Battle" concept could be established relatively quickly, incorporating capabilities from nations with limited defense budgets. Drawing on existing commercial technologies, the proposed approach relies on millimeter-wave radio for communication within the mesh and comparatively simple sensors based on commercial technology. This infrastructure could also incorporate advanced manufacturing techniques like 3D printing, leading to a significant decrease in precision-guidance costs. 9, 13, 16. The US is actively pursuing the Replicator initiative with a clear objective. To maximize benefits for NATO, US leaders should consider partnerships between European defense industries and US companies. Underinvestment and Ukraine support needs have left NATO's weapon stockpiles below desirable levels, despite sustainment being crucial in a potential high-intensity conflict with Russia. Kramer, "NATO Deterrence and Defense: Military Priorities." As Replicator advances, the US should evaluate multinational efforts, such as a US-led consortium with its commercial partners, to build key capabilities for NATO deterrence and defense. B. SEAD: A complex multimodal operation. Suppression of enemy defenses (SEAD) is vital for ground maneuver success. Russia's poor performance in Ukraine partly stems from not conducting effective SEAD campaigns. SEAD requires high-end control, including coordinated targeting for fires, has been established through the combined use of commercial and military technologies. This includes offsetting the consequences of degraded civilian critical infrastructures and adapting to realistic combat conditions. The war in Ukraine provides valuable lessons on how large-scale conflicts may unfold. The use of longer-range HIMARS weapons forced Russia to relocate its sustainment operations, resulting in significant delays. NATO must find ways to overcome these challenges, prioritizing dispersed, resilient logistics that can deliver materiel to the right place at the right time. Sustainment will be crucial in future conflicts, with large-scale combat operations requiring a massive logistical lift. However, Ukraine's experience with rear logistic support areas may not be directly applicable to NATO's situation, as no logistics area can be considered safe in a conflict scenario. NATO logisticsians must develop AI capabilities that can provide dynamic rerouting options and advise on the most valuable logistical routes. The increasing availability of sensors and digital information will present challenges and opportunities for logisticsians. AI systems trained to handle such complexity can provide significant benefits, advising on the most valuable logistical routes and other requirements. The US Army's pursuit of "non-commercially dependent distributed logistics" is an example of this effort, with initiatives underway to load and unload ships outside fixed ports. JSEC, established in 2018 and reaching full operational capability in 2021, is responsible for coordinating sustainment during crisis or conflict under SHAPE. Leveraging large-scale NATO exercises, JSEC gathers data on sustainment operations to inform its advisory role with SACEUR. The Reinforcement and Sustainment Network (RSN) is a database of sustainment-related infrastructure assets and laws affecting their utilization and maintenance. However, JSEC's roles and responsibilities remain unclear. To define its role, NATO should task JSEC with building out the RSN. In dynamic MDO fights, this capability will be crucial for flowing forces in theater and consolidating gains. JSEC must also work closely with the private sector to secure critical infrastructure from kinetic and cyber intrusions. The likelihood of Russia or Belarus attacking a NATO nation near their border necessitates thorough planning by NATO. The region from Finland to Poland and the Baltic states requires special consideration due to geographical challenges. While each country has its own military forces, Poland and Finland have significant capabilities. Following Russia's second invasion of Ukraine, the US bolstered its presence in Europe, stationing armored brigade combat teams in Poland and Romania. Despite having substantial multinational forces in the region, NATO still falls short of its Force Model objective, which aims for over 100,000 Tier 1 forces within ten days. Mobility could hinder achieving this full force on time, potentially leaving forward forces outnumbered until reinforcements arrive. It is crucial that national and forward-stationed forces possess the capabilities to execute a successful defensive action while awaiting reinforcement. Effective use of multimodal operations will be pivotal in achieving this goal. Forward forces must be heavily supported by large quantities of standoff weapons, including long-range fires, air-ground munitions, and land-based anti-air capabilities. Cluster munitions and rapidly deployable mine systems are also key elements of defense in high-intensity conflicts. Multimodal ISR capabilities are essential for both forward forces and their supporting units. Unmanned systems are crucial for smaller defending forces, and frontline nations should invest heavily in unmanned aerial and maritime systems to counter potential threats. Given the struggle against low-cost drones demonstrated by both sides in Ukraine, NATO and its member countries should cooperate in developing cheap and reliable counter-UAS technologies. This technological race may be an area of focus for the Defence Innovation Accelerator for the North Atlantic (DIANA), which aims to accelerate defense innovation across the alliance. NATO's DIANA Initiative Aims to Address Military Challenges The DIANA Initiative is a new program launched by NATO in 2023 to support start-ups developing technologies that can address key challenges faced by the alliance's militaries. The pilot year of DIANA focuses on three main areas: undersea sensing, energy resilience, and secure communications. The program seeks to provide grant financing and mentorship to technology start-ups to help them overcome the "valley of death" in technological innovation. This is particularly important for small units and initiatives by the United States. Currently, the US is working on establishing partnerships with satellite companies through contractual agreements, similar to those used by DOD in collaboration with the airline and maritime industries. The civil reserve air fleet (CRAF) serves as a precedent, providing selected aircraft from U.S. airlines that are contractually committed to augment Department of Defense airlift requirements during emergencies. In line with this concept, the US Space Force is developing a commercial augmentation space reserve (CASR) program, which seeks to establish voluntary pre-negotiated contractual arrangements for services like satellite communication and remote sensing to be prioritized for US government use in national security emergencies. While each NATO nation must determine its own framework, the CASR program offers a useful starting point. Key considerations include determining which services can reliably be provided in wartime scenarios, whether existing or planned private-sector constellations can meet these needs, provisions for satellite and ground station replacement, indemnification, and funding levels to incentivize the private sector, accomplish wartime tasks, and undertake planning and training prior to conflict. The US Defense Production Act also provides authority for prioritized provision of services from space companies, exempting them from liabilities, which would be more desirable through voluntary programs like CASR. NATO's new force model focuses on Europe and aims to counter Russia with over 100,000 Tier 1 forces within ten days and about 200,000 Tier 2 forces in around ten to thirty days. However, how multimodal operations will fit into this approach is unclear. Implementing these operations might require reforming or creating organizations that can effectively combine physical and informational power across different domains. The US Department of Defense has made efforts toward this goal through initiatives like the Advanced Battle Management System, Project Convergence, and Project Overmatch. Yet, these endeavors are still in development, with some reports indicating no capabilities have been delivered to date. NATO could incorporate the concept of multimodal task forces being developed by the US Army into its wartime planning, such as the activated 2nd Multi-Domain Task Force within the European Command. This force recently completed an exercise validating modernization efforts across various domains. The US Army is reorganizing its forces to focus on multimodal operations (MDO), which involve synchronizing effects from land, air, sea, space, and cyber to defeat an adversary. This effort aims to enhance the Army's capability to prevail in high-intensity battles. The creation of multimodal task forces is part of this process, with the goal of building new organizational capabilities that can integrate various domains. These task forces will be designed to support the synchronization and integration of MDO operations undertaken by higher echelons. In a similar vein, NATO should undertake efforts comparable to those being undertaken by the US Army, establishing for its ground forces a theater-corps-division construct and multimodal task forces to coordinate capabilities from all domains. A multitiered approach that plays to the relative strengths of different nations due to geography and economics is necessary, taking into account realistic economic issues surrounding defense budgets. NATO nations face significant challenges in allocating resources to bolster their defense capabilities following Russia's invasion of Ukraine, while navigating ongoing economic constraints posed by the COVID-19 pandemic. The alliance has agreed to allocate 2% of its GDP towards defense spending, but effective utilization of these funds will be crucial in meeting diverse military requirements. A tiered approach to Modernization and Acquisition (MDO) can help reconcile economic limitations with enhanced capabilities. Not all member states require identical capabilities, as smaller countries should prioritize low-cost, attributable solutions like those outlined in the Replicator initiative, whereas frontline nations should focus on proximal-capable assets that can be employed by dispersed units. Larger nations can invest in more expensive platforms, while a balanced mix of both is necessary for maximum effectiveness. The acquisition process must consider several key factors, including US-led MDO initiatives and regional defense planning strategies outlined in the five-step NATO Defense Planning Process (NDPP). Countries should align their purchases with the NDPP's phased approach, which includes determining requirements, apportioning resources, facilitating implementation, and reviewing results. This report recommends seven potential capability areas for near-term focus during the requirements determination process. Capability Requirements for NATO's Alliance - A Crucial Step Towards MDO Adoption NATO's Allied Command Transformation and Allied Command Operations strategic commands are leading steps two and three in the process of Modernization through Acquisition (MDO). In a budget-constrained environment, the third step will be critical to successful adoption of MDO. ACT and ACO must take a strategic view to deconflict acquisitions, coordinate training, and develop collective capabilities iteratively. The Alliance should focus on harmonizing national and Alliance processes using the NATO Defense Planning Process. This will ensure that acquisition mechanisms are coordinated to achieve mass production in domains such as air, land, sea, cyber, and space. MDO requires communication and timing across these domains, which is a complex undertaking requiring significant doctrine and training. Countries should ensure that testing and experimentation inform their acquisitions process. Instead of planning for 90% solutions, they should iterate and exercise capabilities in simulated combat settings to inform adoption. The US Army's Project Convergence is an example of this approach, repeatedly getting technologies into the hands of soldiers to test them in combat environments. This iterative approach would benefit the Alliance by allowing continuous adoption of newer technologies tied to warfighting needs based on tactical and operational experimentation. NATO nations should exercise capabilities like GIS Arta in multilateral, multimodal environments to see their impact on the battlespace. To realize its vision for an MDO-enabled Alliance, NATO must prioritize the adoption and integration of capabilities that enhance its defense and deterrence posture across domains. Near- and medium-term capabilities will accelerate combined all-domain operations with agility and in unison, ensuring the advantage remains tilted in favor of the transatlantic community and democratic values. Distinguished experts from the Atlantic Council's Scowcroft Center for Strategy and Security have made significant contributions to shaping the report on security challenges facing the North Atlantic Alliance. These include Gordon Roddhan, a former associate director of the Transatlantic Security Initiative, and Franklin D. Kramer, a distinguished fellow with extensive experience in defense policy. Kramer has held senior roles in two administrations, including assistant secretary of defense for international security affairs, overseeing global policy initiatives. Ann Marie Daley, a nonresident senior fellow at the Transatlantic Security Initiative, previously served as a senior advisor to the assistant secretary of defense for international security affairs and currently conducts research at the RAND Corporation. Joslyn Brodfuehrer, an assistant director with the Transatlantic Security Initiative, supports efforts to strengthen the transatlantic alliance against emerging threats. Her work builds on her previous experience as a program assistant at the National Endowment for Democracy's International Forum for Democratic Studies. The Transatlantic Security Initiative plays a crucial role in shaping the debate on key security challenges facing the North Atlantic Alliance and its partners, with a focus on maintaining regional stability and countering emerging threats.

Multi domain operations concept. Multi domain operations indian army. Multi domain operations in indian context. Multi domain operations definition. Multi domain operations 2028. Multi domain operations army doctrine. Multi domain operations aviator. Multi domain operations doctrine. Multi domain operations uk. Multi domain operations group. Multi domain operations ppt. Multi domain operations pretest. Multi domain operations army. Multi domain operations aviator tech school. Multi domain operations us army.