Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

NATO MULTIDOMAIN OPERATIONS: NEAR- AND MEDIUM-TERM PRIORITY INITIATIVES

Franklin D. Kramer, Ann M. Dailey, and Joslyn A. Brodfuehrer

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

NATO MULTIDOMAIN OPERATIONS: NEAR- AND MEDIUM-TERM PRIORITY INITIATIVES

Franklin D. Kramer, Ann M. Dailey, and Joslyn A. Brodfuehrer

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The Scowcroft Center's Transatlantic Security Initiative brings together top policymakers, government and military officials, business leaders, and experts from Europe and North America to share insights, strengthen cooperation, and develop innovative approaches to the key challenges facing NATO and the transatlantic community.

Table of Contents

FOREWORD

As NATO ramps up preparations for its 75th Anniversary Summit in Washington in July 2024, the world's most successful military alliance will have much to celebrate. Russia's full-scale invasion of Ukraine—an assault on the rules-based order intended to weaken and divide NATO—instead made the Alliance larger and stronger than ever. The admission of Finland and anticipated entry of Sweden bring NATO even closer to Russia's doorstep. Members bolstered NATO's posture in Europe with a new Force Model and suite of defense plans commensurate with the spectrum of threats. And after decades of underinvestment, nations on both sides of the Atlantic seem to have awoken to the need for a reinvigorated defense-industrial base.

But these causes for celebration are stacked against a threat environment that continues to present enormous challenges to transatlantic security and defense. Allies on NATO's eastern frontier, now facing the reality of protracted conflict in Ukraine, are staring down a Russian adversary that shows no signs of backing down. Though its land forces are severely depleted, Russia's air and strategic forces—as well as its naval forces outside the Black Sea—remain largely untouched. Moreover, post-war Russia could reconstitute its land-based warfighting capabilities within three to five years. The Alliance must also come to terms with challenges emanating from beyond its borders and outside the conventional warfighting arena, as demonstrated by the coercive behavior of Xi Jinping's China, increasing cyber threats below the threshold of war, and recent proliferation of crises that threaten the stability of NATO's southern neighborhood.

In this moment of uncertainty and unprecedented geopolitical contestation, maintaining NATO's warfighting advantage over adversaries will hinge upon the Alliance's continued modernization and ability to operate across domains at speed and scale. Today's battlespace is increasingly connected—combined all-domain operations provide a vehicle for enhanced deterrence and defense, equipping NATO with the capacity to outmaneuver competitors with the coordinated execution of multiple, mutually reinforcing activities across air, space, land, sea, and cyberspace. Although NATO recognizes the value of such an approach, the Alliance and its constituent nations have yet to agree on what multidomain operations (MDO) are, changes they will necessitate in the NATO force structure, and the reforms, investments, and exercises needed to fully operationalize the concept.

The following report seeks to inform this process, offering recommendations for targeted investments that nations can pursue in the near and medium terms to accelerate NATO's transformation into an MDO-enabled warfighting machine. Rather than provide a comprehensive assessment of all capabilities that will be important for a future multidomain fight, the paper prioritizes *attainable* capabilities and approaches—ranging from sensor-shooter networks to artificial intelligence (AI)-enabled agile logistics—that will be critical to MDO and in many cases have proven utility based on preliminary lessons learned from the war in Ukraine, but do not require massive budget outlays or decades-long acquisition processes. Understanding that not all capabilities recommended will be practicable for all allies, the paper concludes with a framework for thinking about platforms NATO countries large and small can acquire to complement existing US initiatives and contribute meaningfully to interallied efforts to conduct adaptable multidomain operations for the twenty-first century.

Due to its focus on capabilities with the capacity to effectuate near-immediate impact, this paper leaves out a number of more expensive, more exquisite, and more politically charged capabilities that are currently dominating NATO's Defense Planning Process—all of which would benefit from an in-depth, follow-on treatment to measure added value against investment. This includes a NATO-wide integrated air- and missile-defense system (IAMDS), a reinforced NATO command-and-control (C2) architecture and battle-management system capable of supporting MDO, and manned air platforms. Somewhat counterintuitively, the utility of these capabilities is proven by their near absence in the war in Ukraine. Because neither side achieved air dominance, the battlefield resembles the trenches of World War I, with a few technological upgrades. Though Ukraine had capable air defenses in the run-up to the war, it has needed to cobble together "FrankenSAMS" to protect its cities and frontline forces. And Russia's lack of assured C2 hastened the collapse of its initial offensive and led to the deaths of dozens of Russian officers. These capabilities will be critical in a future fight, but NATO nations already know this and have begun to pursue them accordingly.

Defending every inch tomorrow will ultimately come down to the investments NATO makes in its ability to execute military operations across domains today. This report charts a concrete path forward for NATO, providing a selective, prioritized set of MDO recommendations on matters not already under active pursuit, and which could be accomplished in the near to medium term with multiplying effects for allied force posture as NATO heads into its seventy-fifth year. Progress on this matter could be a key deliverable for the NATO Summit—in the meantime, the NATO Defense Planning Process is moving forward, and allocation decisions will continue to be made.

Matthew Kroenig

INTRODUCTION

This issue brief sets forth seven priority initiatives focused on NATO multidomain operations (MDO). Implementing these near- and medium-term initiatives—each of which could be accomplished in one to five years—would substantially enhance NATO's deterrence and defense capabilities in support of NATO's recently approved regional plans. Taken together, the proposed actions provide a framework as well as initial steps for an MDO construct across the full spectrum of the NATO-recognized war-fighting domains of air, land, maritime, cyber, and space. Utilizing capabilities available in the near and medium term will significantly increase NATO's ability to fight as a multination coalition. When approaching the technology acquisition and capability initiatives described in this report, individual nations should be guided by the tasks in the regional plans as well as their own geography and economic capabilities. Not all nations need all capabilities, and NATO should utilize its Defense Planning Process[1] to generate a multitiered approach that would take account of the relative military and fiscal capacities among NATO nations.

Specifically, NATO and member nations should establish:

1. Low-cost multidomain surveillance and sensor-shooter networks utilizing unmanned aerial, ground, and maritime capabilities.
2. Multidomain capabilities for suppression of enemy air defenses.
3. Integrated cyber and kinetic offense, focused against adversary logistics and war-supporting infrastructures; and government and private-sector cyber defense, focused on support to militarily critical infrastructures.
4. Dynamic sustainment capabilities, including the use of artificial intelligence (AI), to ensure logistical effectiveness during high-intensity conflict.
5. MDO support for forward-deployed forces to assure survivability and lethality in the initial stages of conflict.
6. Assured provision in wartime of the private-sector space capabilities that are part of NATO's Alliance Persistent Surveillance from Space initiative.
7. Multidomain task forces (MDTFs) to coordinate and integrate capabilities across domains.

I. NEAR- AND MEDIUM-TERM MDO CAPABILITIES

MDO is far from a new concept. The Air-Land Battle, for example, was a major element of NATO's Cold War deterrence and defense doctrine.[2] Intelligence, surveillance, and reconnaissance (ISR) capabilities from multiple sensors, including air and space, have long supported the striking elements of the force in sensor-to-shooter kill chains. The value of establishing a near- and medium-term NATO MDO construct derives from the availability of new or enhanced capabilities to accomplish three key war-fighting tasks more quickly: *Sensing* to develop a prompt and accurate picture of the battlespace, *command and control* to rapidly and securely pass this picture of the battlespace across the strategic, operational, and tactical levels of conflict, and kinetic and nonkinetic *fires* to effect an outcome on the adversary.[3]

As background for the seven priority initiatives recommended in section II of this report, the discussion below sets forth:

- The status of planning for multidomain operations in NATO and its constituent nations, especially the United States.
- MDO lessons learned from the Ukraine-Russia war.
- The US military's current and planned usage of certain commercially available capabilities that can support MDO.

A. Current Planning for Multidomain Operations

Defending every inch of allied territory in an age of unprecedented challenge from malign, near-peer competitors will require NATO and its constituent members to operate at speed and scale across all five operational domains. In recognition of the need for greater synchronization, NATO's Strategic Commands developed the *Alliance Concept for Multi-Domain Operations*.[4] The concept, which was delivered to NATO Headquarters in March 2023, defines MDO as the "orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to create converging effects at the speed of relevance."[5] It effectively outlines NATO military and political leaders' vision for an adaptable, MDO-enabled Alliance capable of outpacing its adversaries.

In recognition of the critical importance of MDO to the Alliance's long-term transformation, NATO Allied Command Transformation (ACT) has identified building an MDO-enabled Alliance as one of

[1] "NATO Defence Planning Process," NATO, March 31, 2022, https://www.nato.int/cps/en/natohq/topics_49202.htm.

[2] John L. Romjue, *From Active Defense to Airland Battle: The Development of Army Doctrine, 1973-1982*, US Army Training and Doctrine Command, TRADOC Historical Monograph Series, June 1984, https://www.tradoc.army.mil/wp-content/uploads/2020/10/From-Active-Defense-to-AirLand-Battle.pdf.

[3] Undergirding all of this will be *survivability*. Given the high intensity of large-scale combat operations, militaries must adopt the technology and tactics, techniques, and procedures to enhance survivability if they are to succeed.

[4] NATO's two strategic commands are Allied Command Operations (ACO), based at Supreme Headquarters Allied Powers Europe (SHAPE), and NATO Allied Command Transformation (ACT). ACT and ACO cooperated closely on the conceptualization of NATO MDO and are now working together on the operational implementation of the concept.

[5] "Multi-domain Operations: Enabling NATO to Out-pace and Out-think Its Adversaries," NATO ACT, July 29, 2022, https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/#:~:text=The%20NATO%20'working'%20definition%20of,at%20the%20speed%20of%20relevance%E2%80%9D.

its strategic priorities for 2023.[6] NATO ACT, in close cooperation with NATO's Strategic Warfighting Command, strives to enhance the Alliance's ability to conduct coordinated and data-driven military operations across domains, with its MDO Implementation Team supporting operationalization of the MDO concept through experimentation, training and exercises, war-gaming, and capability development intended to "[create] both the mind-set and means for military and non-military capabilities to synchronize seamlessly" across domains.[7] NATO ACT, for example, recently signed a memorandum of understanding with the Latvian Ministry of Defense that will allow member nations to conduct operational experiments and test tactical research and development initiatives at the Baltic country's Ādaži military base.[8] In parallel with ACT's efforts, the Supreme Allied Commander Europe (SACEUR) has created an MDO cell at ACO's headquarters in Mons, Belgium. Yet, despite developments like these, most of the Alliance's efforts over the past year have been oriented around definitional and conceptual alignment.[9] While useful, what is missing are concrete, compounded steps toward developing and integrating attainable capabilities and approaches needed to build readiness, transform NATO's force structure, and effectuate combined multidomain operations at speed and scale.

Within the Alliance, some individual nations have begun to embrace and implement multidomain operations, though it is being done unevenly at the national level and without consistent coordination or direction from NATO. Certain nations, like the United Kingdom, have concentrated their efforts on building conceptual frameworks for the integration of capabilities, while others have begun exercises and undertaken initiatives to prepare forces to combat the full spectrum of threats in a multidomain warfighting scenario. French Armed Forces—along with participating nations—concluded the Orion exercise in May 2023, a multiphase drill culminating in the synchronous operation of capabilities such as tactical vehicles, unmanned aerial systems, and spaceborne sensors in response to a scenario simulating multidomain conflict in the future battlespace.[10] Canada has embarked on what it calls an Agile Pan-Domain Command and Control Experimentation Endeavour (APCCXe) that leverages data analytics and AI-enabled tools to test multidomain situational awareness.[11] And smaller member states, led by the Portuguese, rallied under the banner of exercise Real Thaw 2023 (RT23) earlier this year to test their interoperability and capacity to conduct combined operations.[12]

Despite increased attention on enhancing multidomain readiness among allies on both sides of the Atlantic, most member states are outpaced by the United States. The US Department of Defense's joint warfighting concept (JWC)[13] is a US attempt to make sense of the increasingly connected operational environment and functions as a roadmap for how the joint force will operate across all domains now and in the future.[14] The operational concept is threat-informed and intended to drive the future of US warfighting, envisioning a networked "kill web" connecting sensors and fires across domains and between the armed forces to bolster the US ability to prevail in a highly contested fight with adversaries.[15] What sets the United States apart from other allies, however, are its efforts to operationalize this concept and integrate MDO approaches and capabilities at the operational and tactical level.

Ongoing US efforts to coordinate synchronous activities are so far organized around the JWC and enabled by the Combined Joint All-Domain Command and Control (CJADC2) strategy, which the Defense Department describes as "actions to empower our Joint Force Commanders with the capabilities need-

[6] "Ongoing Military Transformation, Leading to NATO 2030—Multi-domain Operations, Deterrence and Defence, Improved Understanding," NATO ACT, March 22, 2023, https://www.act.nato.int/article/ongoing-military-transformation-leading-to-nato-2030-multi-domain-operations-deterrence-and-defence-improved-understanding/.

[7] "Ongoing Military Transformation," NATO ACT.

[8] Elisabeth Gosselin-Malo, "NATO to Test 5G Capabilities in Latvia with Virtual Reality, Drones," *Defense News*, August 31, 2023, https://www.defensenews.com/global/europe/2023/08/31/nato-to-test-5g-capabilities-in-latvia-with-virtual-reality-drones/.

[9] The definitional issue is illustrated by differences within and among allies. While the US Department of Defense (DOD) uses JADO (joint all domain operations) doctrinally, the US Army has doctrinally used MDO (multidomain operations). Canada favors pandomain operations, while other NATO members and NATO as a whole use MDO. NATO should adopt an official definition of MDO and take a decision at the level of the NATO Military Committee to designate MDO as the overarching warfighting concept for the Alliance. This, combined with the delineated tasks outlined in NATO's new regional defense plans, would provide a direction, scope, and prioritization for NATO doctrine, force posture, training, and procurement in the wake of Russia's full-scale invasion of Ukraine. However, in the near and medium term, the seven initiatives described in this issue brief would substantially enhance NATO's deterrence and defense capabilities.

[10] Vivienne Machi, "French Forces Prep for Final Phase of Major Multidomain Exercise," *Defense News*, April 14, 2023, https://www.defensenews.com/global/europe/2023/04/14/french-forces-prep-for-final-phase-of-major-multi-domain-exercise/.

[11] "Joint Experimentation at the Canadian Joint Warfare Centre," Government of Canada, August 10, 2023, https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2023/08/joint-experimentation-canadian-joint-warfare-centre.html.

[12] "Multinational Exercise Real Thaw Begins in Portugal," NATO Allied Air Command, March 2, 2023, https://ac.nato.int/archive/2023/multinational-exercise-real-thaw-begins-in-portugal.

[13] John Harper, "US Military Publishes New Joint Warfighting Doctrine," *DefenseScoop*, September 13, 2023, https://defensescoop.com/2023/09/13/us-military-publishes-new-joint-warfighting-doctrine/. The current JWC was quietly published on August 27, but is not publicly available.

[14] Gen. Mark A. Milley, "Strategic Inflection Point: The Most Historically Significant and Fundamental Change in the Character of War Is Happening Now—While the Future Is Clouded in Mist and Uncertainty," *Joint Force Quarterly 110* (July 2023), https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-110/Article/Article/3447159/strategic-inflection-point-the-most-historically-significant-and-fundamental-ch/.

[15] Lt. Col. Brittany Lloyd and 2nd Lt. Jeremiah Rozman, "Achieving Decision Dominance through Convergence: The U.S. Army and JADC2," Association of the United States Army, February 2, 2022, https://www.ausa.org/publications/achieving-decision-dominance-through-convergence-us-army-and-jadc2.

ed to command the Joint Force across all warfighting domains and throughout the electromagnetic spectrum to deter, and, if necessary, defeat any adversary at any time and in any place around the globe."[16] To implement the JWC, each military service is undertaking multiple different initiatives to build the capacity of the joint force to conduct combined and joint operations across domains.[17] Four key initiatives include:

- **Advanced Battlefield Management System (ABMS)**: The Air Force's ABMS seeks to create an Internet of Things (IoT) that uses AI to integrate Air Force and Space Force data to accelerate decision-making in the battlespace.[18] Five on-ramp exercises have been performed since the system's origination, with the next generation of efforts organized around supplementing the ABMS with what the Department of the Air Force (DAF) calls the DAF Battle Network—a new structure that Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics Andrew Hunter believes will facilitate service integration into the DOD's joint all-domain command and control endeavor.[19]
- **Project Overmatch**: Although the Navy has released few details about Project Overmatch, open-source reporting indicates that its contribution to CJADC2 includes enhancing software capabilities to bolster connectivity among systems.[20] The 2023 phase of the project will include activities associated with a carrier strike group, according to a *Navy Times* report.[21]
- **Project Convergence**: Run by the Army Futures Command, Project Convergence aims to build sensor-shooter networks enabled with AI capabilities to equip commanders with a more accurate picture of their operating environment and speed decision-making processes.[22] Annual experiments have been held since 2020 to test the Army's ability to integrate capabilities across the joint force,[23] with the 2024 iteration to focus on theater-level experimentation to assess whether and how effectively its network of sensors is connecting threats with the capabilities needed to eliminate them.[24]
- **Stand-In Forces**: The US Marine Corps released *A Concept for Stand-In Forces* in December 2021 under the banner of *Force Design 2030*.[25] Aligned with the JWC and intended to enhance integrated deterrence, the concept envisions Marine stand-in forces (SIF)—defined as "small but lethal, low signature, mobile, relatively simple to maintain and sustain forces designed to operate across the competition continuum within a contested area"—that can be employed to improve the situational awareness of the joint force, complete kill webs, and ultimately disrupt and deter potential adversaries.[26] SIF can be composed of personnel from each service, as well as allies and partners, making them an inherently joint effort and a conduit for enhanced interallied cooperation.

Against this backdrop and with the United States as the essential warfighting backbone of the Alliance, NATO's ability to execute effective military operations will require its members both to build around the United States' progress and to work together to integrate their national approaches to MDO in a way that complements their comparative advantages.

[16] *Summary of the Joint All-Domain Command & Control (JADC2) Strategy*, DOD, March 2022, 1, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.

[17] Charles McEnany, "Multi-domain Task Forces: A Glimpse at the Army of 2023," Association of the United States Army, March 2, 2022, https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035. The US Army describes multidomain operational concepts more comprehensively than any other service branch in *Field Manuel No. 3-0* (FM 3-0). Among other initiatives, the Army plans to operationalize MDO by fielding five Multi-Domain Task Forces (MDTFs)—defined as "theater-level, multi-domain maneuver elements that synchronize long-range precision effects (LRPE) . . . with long-range precision fires (LRPF)" to help forces win in the future battlespace.

[18] John Hoehn, "Advanced Battle Management System (ABMS)," Congressional Research Service, last updated February 15, 2022, https://sgp.fas.org/crs/weapons/IF11866.pdf.

[19] Sean Carberry, "Special Report: Air Force Reorganized to Tackle JADC2 Complexities," *National Defense*, July 12, 2023, https://www.nationaldefensemagazine.org/articles/2023/7/12/air-force-reorganizes-to-tackle-jadc2-complexities.

[20] Josh Luckenbaugh, "Special Report: Navy Testing Secret JADC2 Technologies," *National Defense*, July 13, 2023, https://www.nationaldefensemagazine.org/articles/2023/7/13/navy-testing-secret-jadc2-technologies.

[21] Geoff Ziezulewicz, "New in 2023: Project Overmatch Heads to Sea," *Navy Times*, January 5, 2023, https://www.navytimes.com/news/your-navy/2023/01/05/new-in-2023-project-overmatch-heads-to-sea/.

[22] Andrew Feickert, "The Army's Project Convergence," Congressional Research Service, last updated June 2, 2022, https://sgp.fas.org/crs/weapons/IF11654.pdf.

[23] Feikert, "The Army's Project Convergence." The project is intended to "take the service's big ideas for future warfare and test them in the real world." Experiments have, for example, challenged the Joint Force to test joint all-domain situational awareness, conduct a joint fires operation, and facilitate AI-enabled reconnaissance missions.

[24] Jen Judson, "Army Sets Sights on 2024 for Next Project Convergence," *Defense News*, February 7, 2023, https://www.defensenews.com/land/2023/02/07/army-sets-sights-on-2024-for-next-project-convergence/#:~:text=The%20next%20Project%20Convergence%20will,include%20tackling%20more%20challenging%20threats.

[25] *Force Design 2030: Annual Update*, US Marine Corps, June 2023, https://www.marines.mil/Portals/1/Docs/Force_Design_2030_Annual_Update_June_2023.pdf. *Force Design 2030* provides a roadmap for the Marine Corps' transformation into a "more agile, efficient, and technologically advanced force to meet the challenges of the future." Stand-in forces, littoral operations, force sizing, training, and cooperation with allies are all prioritized under this strategy to bolster the services' ability to deter and defend.

[26] "A Concept for Stand-in Forces," US Marine Corps, December 2021, https://www.hqmc.marines.mil/Portals/142/Users/183/35/4535/211201_A%20Concept%20for%20Stand-In%20Forces.pdf.

Operationalizing NATO's MDO concept and bolstering the connective tissue that links the yet largely uncoordinated efforts of allies will be the most important lines of effort for the Alliance to pursue in the near and medium terms to build itself into an MDO-enabled warfighting machine. Organization and coordination of the efforts of NATO's thirty-one member states will be a necessary factor for the Alliance to effectuate tactical operations across domains. A lack of investment into interallied coordination of MDO will undermine NATO's new defense plans and broader efforts to modernize its force model and communications infrastructure—putting the North Atlantic alliance on the back foot before the first strike.

B. Lessons from the Ukraine-Russia War

The ongoing Ukraine-Russia war holds a series of lessons for NATO's MDO activities. In the war, the Ukrainian forces have been able to build and communicate a highly accurate picture of the operational environment, and as a result have been able to establish an effective targeting capability, thereby mitigating Russian quantitative weapons and personnel advantages.

1. Sensing: At the sensing level, Ukraine has combined strategic and tactical intelligence shared by the United States and its European partners with information from their own intelligence apparatus, including open-source (and even crowd-sourced) intelligence to provide their civilian and military leaders informational advantages in the campaign.[27]

An analyst recently described the innovation this way:

> But what's most noteworthy is how Ukrainian conscripts have been able to use *clusters* of commercial and military technologies (interacting technologies like sensors, satellites, machine learning, and quickly updateable software) to network, interact, and create dynamic systems much faster than Russian soldiers can. . . .
>
> Everyone—from the Ukrainian soldier employing weaponized commercial drones to President Volodymyr Zelensky making nation-wide decisions—has relied on an interlinked system to collect, analyze, and translate data into actionable results in civilian neighborhoods or on the battlefield. With the help of NATO allies and open source companies outside Ukraine, the armed forces have leveraged both public and private technologies to create a data-driven command-and-control system through four dimensions—collection, connection, analysis, and action.[28]

A critical element for Ukraine's sensing operations has been its ability to combine military and commercial capabilities. As set forth in a prior Atlantic Council report (by one of the brief's authors),[29] Ukraine has developed, for instance, the Delta Situational Awareness Systems, which an intelligence firm described as providing "a comprehensive picture of the current battle space displayed and summarised on a user-friendly digital map by collecting data from sensors and open and secret sources."[30] A press report says it "integrates real-time intelligence data from multiple sources and provides real-time monitoring of the battlefield for commanders of different levels."[31]

A key aspect of Delta is that it utilizes available commercial technology to provide the information to users as the system "is ready to use on laptops, tablets, or mobile phones."[32]

2. Communications: Ukraine's military capabilities have relied heavily on communications facilitated by the commercial satellite company Starlink, which is operated by SpaceX. This has been well-described by Emma Schroeder and Sean Dack:

> Starlink, a network of low-orbit satellites working in constellations operated by SpaceX, relies on satellite receivers no larger than a backpack that are easily installed and transported. Because Russian targeting of cellular towers made communications coverage unreliable . . . the government "made a decision to use satellite communication for such emergencies" from American companies like SpaceX. Starlink has proven more resilient than any other alternatives throughout the war. Due to the low orbit of Starlink satellites, they can broadcast to their receivers at relatively higher power than satellites in higher orbits. There has been little reporting on successful Russian efforts to jam Starlink transmissions.[33]

In the wake of news that SpaceX CEO Elon Musk proscribed Starlink accessibility in a way that hindered a Ukrainian attack,[34] the Ukraine conflict also demonstrates the potential drawbacks should the military become overly reliant on private companies

[27] Neveen Shaaban Abdalla et al., "Intelligence and the War in Ukraine: Part II," *War on the Rocks*, May 19, 2022, https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-2/.

[28] Audrey Kurth Cronin, "Open Source Technology and Public-private Innovation Are the Key to Ukraine's Strategic Resilience," *War on the Rocks*, August 25, 2023, https://warontherocks.com/2023/08/open-source-technology-and-public-private-innovation-are-the-key-to-ukraines-strategic-resilience/.

[29] Franklin D. Kramer, "NATO Deterrence and Defense: Military Priorities for the Vilnius Summit," Issue Brief, Atlantic Council, April 18, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-summit-military-priorities/.

[30] Oscar Rosengren, "Network-centric Warfare in Ukraine: The Delta System," Grey Dynamics, February 3, 2023, https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/.

[31] "Ukraine to Implement Delta Situation Awareness System in Defense Forces," *Euromaidan Press*, February 4, 2023, https://euromaidanpress.com/2023/02/04/ukraine-to-implement-delta-situation-awareness-system-in-defense-forces/.

[32] Rosengren, "Network-centric Warfare in Ukraine."

[33] Emma Schroeder and Sean Dack, *A Parallel Terrain: Public-private Defense of the Ukrainian Information Environment,* Cyber Statecraft Initiative and Digital Forensic Research Lab, Atlantic Council, 2023, 16.

[34] Tara Copp, "Elon Musk's Refusal to Provide Starlink Support for Ukraine Attack in Crimea Raises Questions for Pentagon," Associated Press via PBS *NewsHour*, September 11, 2023, https://www.pbs.org/newshour/economy/elon-musks-refusal-to-provide-starlink-support-for-ukraine-attack-in-crimea-raises-questions-for-pentagon#:~:text=(AP)%20%E2%80%94%20SpaceX%20founder%20Elon,purchases%20could%20be%20used%20in.

for low-earth orbit-enabled communications if there is not assured access to the capability. While this concern is valid and overreliance certainly would be problematic, governments should continue both their investments on more exquisite satellite capabilities while also leveraging commercially available LEO capabilities for communications and other capabilities. As discussed below, contracts with private companies should not allow for those companies to unilaterally alter their networks in a way that would negatively impact warfighting capabilities.

3. Command and control and fires: Ukraine's ability to establish effective command and control, including coordinated targeting for fires, has likewise benefited from the combined use of commercial and military technologies that have established highly effective sensor-to-shooter linkages. One key geographic information system based on commercial technology is GIS Art for Artillery (Arta), which links targeting information with strike capabilities so that "forward observers, unmanned aerial systems, or other scout elements can share their observations of an enemy target's location in real time over an encrypted network," which uses "satellite, internet, and radio protocols across a number of devices readily available to all [Ukrainian] echelons."[35]

Another key software-based system is Kropvya, "an intelligence mapping and artillery software populated by information" from unmanned aerial systems and other sources. Forward-deployed tactical units download the software, which is continuously updated and allows them to plot enemy and friendly positions. The system uses short-wave and digital radio stations and is compatible with NATO's security communications standards.[36]

4. Unmanned aerial vehicles: The Ukraine-Russia war has shown the benefit of lower cost unmanned aerial vehicles (UAVs), both for sensing and striking.

Sensing has significantly benefited. In *War on the Rocks*, Audrey Kurth Cronin noted the widespread use and impact of commercial products:

> Individual military units use commercial, off-the-shelf drones like DJI's Phantom 3 or AeroVironment's Quantix Recon to conduct intelligence, surveillance, and reconnaissance missions within a few miles of their positions. Hobbyist drones collect information critical to tactical intelligence requirements, especially for targeting. By May 2022, Ukraine had fielded 6,000 commercial drones to provide surveillance capabilities to military units. A year later they had vastly expanded their "Army of Drones" and the Royal United Services Institute estimated that the Ukrainians were losing 10,000 drones a month.[37]

Low-cost drone capabilities facilitate striking, with information from field brigades sent to military intelligence, according to an *Economist* report:

> Drones target "fuel depots, logistics, ammunition dumps and delivery routes," says Detective, the pseudonym of a drone co-ordinator in Ukraine's military intelligence. "We respond to appeals from our brigades. They tell us they know where Russian arms are being stored, but have no way of hitting them, and they plead with us to help." Detective says much of his recent work has been focused on airfields near Ukraine's borders. This   "might" have included a recent strike that hit a Tu-22m strategic bomber based near Novgorod, he adds with a wink.[38]

Another strike capability is provided by "first person view" drones that are flown by an "operator [who] dons goggles that show a video feed from them as they fly."[39]

> They are assembled by volunteers or by the soldiers themselves from components provided by fundraisers. The simplicity of the electronics and use of commercial components means that they are cheap to make. One Ukrainian-made Pegasus attack drone costs $462 to buy. The larger and more refined SwitchBlade drones that America supplies to Ukraine, which carry only a small antipersonnel warhead, cost $52,000 apiece or more. FPVs' low cost compensates for their relatively low rate of success in destroying targets. Operators put their success rate at 50%-80%, compared with 90% or more for American Javelin anti-tank missiles.[40]

5. Cyber resilience: Cyber resilience to Russian attacks has been critical to Ukraine's military effort (as well as helping support the economy and society more generally). A Scoop News Group report by Elias Groll and AJ Vicens conveys the impact:

> The war has inspired a defensive effort that government officials and technology executives describe as unprecedented—challenging the adage in cybersecurity that if you give a well-resourced attacker enough time, they will pretty much always succeed. The relative success of the defensive effort in Ukraine is beginning to change the calculation about what a robust cyber defense might look like going forward.[41]

[35] Mark Bruno, "'Uber for Artillery'—What Is Ukraine's GIS Arta System?," *The Moloch* (blog), August 24, 2022, https://themoloch.com/conflict/uber-for-artillery-what-isukraines-gis-arta-system.

[36] Seth G. Jones , Riley McCabe, and Alexander Palmer, *Ukrainian Innovation in a War of Attrition*, Center for Strategic and International Studies, February 27, 2023, https://www.csis.org/analysis/ukrainian-innovation-war-attrition.

[37] Cronin, "Open Source Technology and Public-private Innovation."

[38] "Inside Ukraine's Drone War against Putin," *Economist*, August 27, 2023, https://www.economist.com/europe/2023/08/27/inside-ukraines-drone-war-against-putin.

[39] "How Could FPV Drones Change Warfare?," *Economist*, August 4, 2023, https://www.economist.com/the-economist-explains/2023/08/04/how-could-fpv-drones-change-warfare.

[40] "How Could FPV Drones Change Warfare?," *Economist*.

[41] Elias Groll and AJ Vicens, "A Year After Russia's Invasion, the Scope of Cyberwar in Ukraine Comes into Focus," *Cyberscoop*, February 24, 2023, https://cyberscoop.com/ukraine-russia-cyberwar-anniversary/.

The key to success has been the high degree of collaboration between governments—i.e., Ukraine's effectiveness, bolstered by US and United Kingdom support—and the private sector:

> The defensive cyber strategy in Ukraine has been an international effort, bringing together some of the biggest technology companies in the world such as Google and-Microsoft, Western allies such as the U.S. and Britain and social media giants such as Meta who have worked together against Russia's digital aggression.[42]

C. Commercially Based US Defense Capabilities

The United States has undertaken significant efforts in recent years to utilize commercial capabilities in support of military operations.

1. Low-earth orbit satellites: Satellites have long been used for multiple purposes to tie the space domain to the air, land, and maritime domains including ISR; positioning, navigation, and timing; communications; and targeting. A recent fundamental shift can be seen, however, in the expanding US use of low-earth orbit satellites to accomplish the tasks performed by existing higher-orbit satellites. In addition to Starlink (described above), the commercial sensing technologies of satellite companies like Planet, Capella Space, and Maxar, which have proven important in Ukraine's fight, can likewise be used as a complement to the US military's more exquisite sensing."[43]

Commercial capabilities are similarly being increasingly relied upon to meet the military's space-launch requirements. DOD recently used private-sector SpaceX Falcon 9 reusable rockets, which are regularly used for commercial satellites, to launch ten of an expected twenty-eight satellites for defense "low-latency communications" and "missile warning/missile tracking."[44] That space architecture is planned to expand to 163 satellites.[45] Other companies such as Rocket Lab likewise have commercial launch capabilities.[46]

2. Commercially based aerial and maritime surveillance: US Central Command has successfully utilized low-cost unmanned vehicles based on commercial technology for both maritime and aerial surveillance, and has coupled the surveillance with AI capabilities to maximize results. One report described the maritime effort:

> The Navy stood up TF 59 in September 2021 . . . [in a] turn to the private sector [and] . . . within a month, the new unit had begun deploying unmanned, unarmed,camera-laden sea drones linked by artificial intelligence into the Persian Gulf.[47]

The task force has utilized a number of different commercial capabilities including Saildrones and MARTAC's Mantas T12s and T38 Devil Rays. It also has conducted a series of exercises with navies in the Central Command area of responsibility including with Bahrain, Jordan, Kuwait, Qatar, Saudi Arabia, and Israel, with the objective of having regional navies provide eighty such devices by the end of 2023.[48] The net result is a highly effective low-cost capability: "For pennies on the dollar, we can put unmanned platforms out there, we can couple it with artificial intelligence, and we can really get a sense for what's happening," Vice Adm. Brad Cooper told reporters during a Pentagon visit in October 2022. "The end result of that is you simply can advance your capability on orders of magnitude faster by this close connection with industry," he is quoted as saying by *Al-Monitor.*[49]

The Air Force's Task Force 99 similarly utilizes commercially available "small, high-altitude drones linked by [a] mesh network" for air domain awareness.[50] As described by Lt. Gen. Alexus Grynkewich, commander of Air Force Central Command, in a press report, the surveillance capability is enhanced by coupling it with AI:

> Task Force 99 was born out of the idea that if we take unmanned technologies and digital technologies and pair them together, and basically teach the robots and the algorithms to solve some of these problems for us, that it could fill some of those gaps."[51]

3. The Replicator initiative to field attritable autonomous systems at scale: DOD has recently established a new initiative called Replicator. As described by Deputy Secretary Kathleen Hicks in late August, Replicator is intended to "create a new state of the art . . . leveraging attritable, autonomous systems in all domains—which are less expensive, put fewer people in the line of fire, and can be changed, updated, or improved with sub-

[42] Groll and Vicens, "A Year After Russia's Invasion."

[43] Christine H. Fox and Emelia S. Probasco, "Big Tech Goes to War," *Foreign Affairs*, October 19, 2022, 4, https://www.foreignaffairs.com/ukraine/bigtech-goes-war.

[44] "Space Development Agency Successfully Launches Tranche 0 Satellites," DOD, April 2, 2023, https://www.defense.gov/News/Releases/Release/Article/3348974/space-development-agency-successfully-launches-tranche-0-satellites/.

[45] "Space Development Agency Successfully Launches," DOD.

[46] "About Us," Rocket Lab, accessed July 5, 2023, https://www.rocketlabusa.com/about/about-us/.

[47] Jared Szuba, "US Top Middle East Commander Tests New Model of Deterring Iran," *Al-Monitor*, January 3, 2023, https://www.al-monitor.com/originals/2022/12/us-top-middle-east-commander-tests-new-model-deterring-iran.

[48] Szuba, "US Top Middle East Commander Tests New Model."

[49] Szuba, "US Top Middle East Commander Tests New Model."

[50] Szuba, "US Top Middle East Commander Tests New Model."

[51] John Harper, "US Central Command's New Task Force 99 Begins Drone Operations in Middle East," *DefenseScoop*, February 13, 2023, https://defensescoop.com/2023/02/13/us-central-commands-new-task-force-99-begins-drone-operations-in-middle-east/.

stantially shorter lead times."[52] The goal for the next eighteen to twenty-four months is, she said, "to field attritable autonomous systems at scale of multiple thousands, in multiple domains."[53]

While the deputy secretary did not identify particular domains or types of systems, the next section of this report proposes specifics which would build on the Replicator initiative as part of the recommended seven priority initiatives for NATO action.

II. PRIORITY INITIATIVES

NATO deterrence and defense capabilities will be substantially enhanced by implementing the seven initiatives described below. Each of these initiatives can be accomplished in the near or medium term (i.e., one to five years) and each is relatively inexpensive.

A. Low-Cost Surveillance and Sensor-Shooter Networks

Ukraine has made effective use of low-cost, unmanned aerial vehicles in its conflict with Russia, as described above. DOD's Replicator initiative demonstrates that this lesson has been incorporated into the thinking of senior US defense leadership. The rationale is not hard to discern. While the United States and other NATO allies and partners have multiple high-end unmanned capabilities, these systems are costly, as illustrated by the per-copy pricing for the US Gray Eagle ($127 million), Reaper ($28 million), and Global Hawk ($141 million).[54]

Similarly, the US Air Force's plans for sixth-generation uncrewed aircraft like Boeing's MQ-28A Ghost Bat—more commonly known as the "Loyal Wingman"—include the ability to fly alongside F-35s and conduct AI-enabled teaming missions, but likely will entail significant expense (though pricing is as-yet uncertain). According to an estimate by the House of Representatives, the cost could range between $3 million and $25 million per copy.[55] Likewise, the Air Force's acquisition strategy for its Collaborative Combat Aircraft program for high-end uncrewed fighters to be fielded within its Next Generation Air Dominance (NGAD) family of systems is looking to cap costs at no more than $40 million per copy.[56] While there would be value in having those capabilities, the Replicator initiative is also intended to bring valuable capabilities into the force at prices far below those required by current and planned systems—and far more quickly.

As Hicks pointed out, the key for the United States and NATO is to augment exquisite capabilities with less complex and inexpensive systems comparable in broad terms with the weapons systems being utilized in Ukraine. Such low-cost, still-effective unmanned capabilities will add to NATO's ability to enhance ISR, to add mass to the battle, and to establish an offense-defense cost ratio that is in NATO's favor. Importantly, such capabilities can come into the force quite promptly as both their usage in Ukraine and the specified Replicator time frame underscore.

In outlining the initiative, Hicks left open the particular areas of focus, but there are several described below that would have high impact for NATO deterrence and defense.

As a first step, a valuable starting point would be building on the capabilities demonstrated by Central Command's Task Force 59, which focuses on integrating unmanned systems and AI with maritime operations, to establish maritime surveillance networks for the Baltic, Black, and Mediterranean seas. The United States should work with the relevant littoral NATO nations to put such capabilities promptly in place. Cooperative efforts could be undertaken bilaterally, regionally, or in a trisea consortium.

A second effort could focus on ground force lethality. Unmanned aerial vehicles could supply targeting information including through systems like GIS Arta to artillery units or to other UAVs with ground attack capabilities. Tactical unit capabilities could likewise be enhanced by combining video-viewing capabilities for operators of unmanned vehicles providing targeting information.

Above the tactical level, the potential for use of unmanned capabilities is even greater. As RAND Corporation researchers have described in a series of reports, a low-cost, but highly effective sensing and targeting grid can be based on inexpensive UAVs:

> Ongoing developments in robotics and autonomous sensing can enable a force to establish a ubiquitous sensing and targeting grid in contested areas using large numbers of unmanned platforms. If the platforms and other hardware used in the grid can be procured at low cost, such an approach can achieve resiliency through sheer numbers. In the Taiwan Strait, for example, the United States' and Taiwan's forces together could launch hundreds of unmanned drones into the strait and the airspace above it. Each drone would be equipped with one or more sensors, allowing them to collect data via electro-optical, radar, and acoustic means. Using edge processing, these data could be processed onboard each sensor platform. Using automatic target recognition algorithms, the grid itself would determine what types of vessels it has observed. As defending forces launched antiship missiles toward the battlespace, the grid would

[52] "Deputy Secretary of Defense Kathleen Hicks Keynote Address: 'The Urgency to Innovate,' " DOD, August 28, 2023, https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/.

[53] "Deputy Secretary of Defense Kathleen Hicks Keynote Address," DOD.

[54] John R. Hoehn and Paul K. Kerr, "Unmanned Aircraft Systems: Current and Potential Programs," Congressional Research Service, July 28, 2022, 6, 7, 11, https://crsreports.congress.gov/product/details?prodcode=R47067.

[55] Eric Lipton, "A.I. Brings the Robot Wingman to Aerial Combat," *New York Times*, August 27, 2023, https://www.nytimes.com/2023/08/27/us/politics/ai-air-force.html.

[56] Valerie Insinna, "Coming Soon: A US Competition for Sixth-gen Drone Wingman Could Begin in FY24," *Breaking Defense*, September 7, 2022, https://breakingdefense.com/2022/09/coming-soon-a-us-competition-for-sixth-gen-drone-wingman-could-begin-in-fy24/.

> assign a target to each one, communicating the target's latest location to the incoming weapon using the same data links that were used to share information with other platforms within the grid.[57]

While the foregoing describes a Taiwan strait scenario, a third specific NATO activity based on the RAND analysis would be establishing such a UAV-based targeting approach for sea control in the Baltic, Black, and Mediterranean seas.

A fourth NATO effort would be to utilize such a sensing and targeting grid against Russian land forces. The RAND researchers determined that the "same approach [as in a Taiwan scenario] could be employed to support a defense against Russia's invasion, substituting unattended ground sensors for unmanned maritime drones."[58] Utilizing that combination of capabilities would generate a modern "Air-Land Battle" that NATO could relatively promptly put in place. Such an approach would also have the value of including as part of the overall structure capabilities provided by nations with smaller defense budgets, as they would be able to afford lower cost UAVs.

The capabilities that the RAND analyses describe—and that have been proposed by Hicks for the Replicator initiative—are well within reach in the near and medium term, as they rely on commercially available capabilities. Drawing on press and Atlantic Council reports to illustrate how it can work: A targeting mesh would be built on "comparatively simple sensors based on commercial technology"; communication within the mesh "is provided by millimeter-wave (MMW) radio, a technology already widely used for 5G communications."[59] There is even the potential for the commercial sector to utilize, as Ukraine has done,[60] "advanced manufacturing techniques [i.e., 3D printing]" that could lead to an "exponential drop in the cost of precision-guidance technologies."[61]

The United States is pursuing the Replicator initiative with purpose. To maximize the benefits for NATO, US leaders should consider how the European defense industry might partner with US companies. A combination of historical underinvestment and the demands of supporting Ukraine have meant that NATO weapons inventories are far below desirable levels even though sustainment would likely be a key factor in a high-intensity conflict with Russia.[62] As the Replicator initiative moves forward, the United States should evaluate the potential for multinational efforts—for example, by a US-led consortium of nations and its US commercial Replicator partners—to build the types of capabilities described above as key elements of NATO deterrence and defense.

B. SEAD: An Inherently Multidomain Operation

Suppression of enemy air defenses (SEAD) is a key factor for enabling ground maneuver. Russia's failure to conduct a campaign to suppress enemy air defenses in Ukraine is one of the main reasons that it has done so poorly in the war. Part of why Russia did not do this is that SEAD is an incredibly complex mission set that requires not only high-end platforms but also flexible mission planning and tight coordination between different domains in order to achieve effects. In other words, SEAD is inherently an MDO.

The SEAD mission follows a find, fix, track, target, engage, assess (F2T2EA) process that is designed to degrade an adversary's integrated air defense systems (IADS), and which requires use of the electromagnetic spectrum (EMS) as a key maneuver space. The initial finding and fixing efforts require effective ISR. How that is done will depend on a number of factors, including what is being targeted, where the target is, how and whether the target is controlling its electromagnetic emissions (EMCON), time of day, and the weather. In order to find and fix an EMCON target, it is necessary to get it to respond to some sort of stimulus so it can be seen (i.e., the target needs to be lit up). Doing this against IADS will often require the use of cyber and/or space capabilities. SEAD also requires an ability to discriminate between false EMS signals and legitimate targets. Tracking and targeting would generally then be taken over by other assets, usually manned or unmanned aerial systems, which can either engage the platforms themselves or pass a more refined track on to other platforms. This could include ground,[63] air,[64] and sea-based systems.[65] The final step in the F2T2EA process—under-

[57] David A. Ochmanek et al., *Inflection Point: How to Reverse the Erosion of U.S. and Allied Military Power and Influence* (Santa Monica, California: RAND Corporation, 2023), 28-29, https://www.rand.org/pubs/research_reports/RRA2555-1.html.

[58] Ochmanek et al., *Inflection Point: How to Reverse the Erosion*, 29.

[59] David Hambling, "Low-Tech, Unkillable 'Mesh' of Targeting Drones Could Help Destroy a Chinese Fleet Invading Taiwan," *Forbes*, September 21, 2021, https://www.forbes.com/sites/davidhambling/2021/09/21/low-tech-targeting-mesh-drones-could-tip-the-odds-against-a-chinese-fleet-invadingtaiwan/?sh=2cf199084b45.

[60] "Ukraine's Latest Weapons in Its War with Russia: 3D-printed Bombs," *Economist*, August 1, 2023, https://www.economist.com/science-and-technology/2023/08/01/ukraines-latest-weapons-in-its-war-with-russia-3d-printed-bombs.

[61] T. X. Hammes, "Game-changers: Implications of the Russo-Ukraine War for the Future of Ground Warfare," Atlantic Council, April 3, 2023 , 9, 13, 16, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/game-changers-implications-of-the-russo-ukraine-war-for-the-future-of-ground-warfare/.

[62] Kramer, "NATO Deterrence and Defense: Military Priorities."

[63] Ground-based, long-range artillery systems such as the currently employed High-Mobility Artillery Rocket System (HIMARS) have been used to great effect in Ukraine when paired with the Guided Multiple Launch Rocket System (GMLRS). HIMARS also can fire a single Army Tactical Missile System (ATACMS) missile with a range of 300 kilometers. In the near future, this also could include the Precision Strike Missile (PrSM), which will range 499+ km.

[64] Air systems could include the Joint Air-to-Surface Strike Missile (JASSM), which is a cruise missile whose range with an extended range variant exceeds 525 miles, or the long-range anti-ship missiles (LRASM), which is precision guided and can target maritime missile defense platforms.

[65] The Tomahawk Land Attack Cruise Missile (TLAM) is a ship- or submarine-launched cruise missile.

taking battle-damage assessment—again can be conducted by a variety of capabilities in a variety of domains, ranging from maritime and air to space, cyber, and land.

Currently, the United States is the single nation that regularly trains and exercises SEAD (though China has recently tried). No other NATO nation can conduct SEAD, nor could NATO without US capabilities. However, NATO nations could usefully augment US capabilities as several possess or are in the process of acquiring high-end capabilities that can engage enemy IADS, including high-end aircraft (F-35), artillery (the High-mobility Artillery Rocket System, or HIMARS) and cruise missiles (e.g., Storm Shadow, SCALP-EG, Taurus) which can make significant contributions to the SEAD mission. Furthermore, nations that may not have higher-end platforms capable of contributing to the "engage" portion of the F2T2EA process still can invest in cyber, ISR, and/or special forces capabilities that would contribute to all of the other steps in the process.

Undertaking SEAD as a combined NATO mission—as opposed to a US-only effort—will require extensive training and exercising, but the process could be accomplished within the near-to-medium term and therefore would be of high value in the event of a conflict with Russia through an expanded NATO capacity for SEAD. Supreme Headquarters Allied Powers, Europe should organize the necessary training and exercising to achieve the requisite capability. Additionally, while the training and exercising process is underway, the nations that will be engaged should continue to ensure adequate stockpiles of munitions and other capabilities that can be used for a SEAD mission, including the Guided Multiple Launch Rocket System (GMLRS), Army Tactical Missile System (ATACMS) (and Precision Stike Missile in future), Joint Air-to-Surface Strike Missile (JASSM), small diameter bombs (or SDB) for less advanced air defense platforms, and joint direct attack munitions (JDAMS).[66]

C. Cyber: Multidomain Offense and Defense

1. Cyber offense: Multidomain cyber offense can have both tactical and operational/strategic aspects. At each of the tactical and operational levels, cyber should not be considered in isolation, but rather commanders generally should look to rely on the "effective integration of kinetic and cyber strike capabilities," according to a NATO Cooperative Cyber Defence Centre of Excellence paper.[67]

Like other strike capabilities, cyber relies on effective ISR and, of course, has its own inherent ISR capabilities. However, cyber offense can also utilize ISR derived from UAVs deployed in battlespace or properly equipped LEO satellites. A multidomain unit could, for instance, "make use of either tactical or strategic intelligence assets (such as RF kit on the ground or a satellite) to gain access to a network and facilitate delivery of a cyberattack."[68] And the effect could be tactical or strategic: disrupting a surface-to-air battery or theatre-level combat and control capacity.[69]

The operational value of cyber offense capabilities includes cyber's ability to attack an adversary's critical infrastructure. Effective targeting of cyber capabilities, which "can be targeted in tandem with kinetic military action to yield significant effects,"[70] would include attacks against adversary logistics, communications networks, rear area military operations, and war-supporting industry, as well as against civilian critical infrastructures such as energy and transportation supporting those and other military capabilities.[71]

To prepare its capacity for cyber offense, NATO set up a Cyberspace Operations Center in Belgium to "support military commanders with situational awareness" for operations and missions including "operational activity in cyberspace, ensuring freedom to act in this domain and making operations more resilient to cyber threats."[72]

The actual implementation of NATO's cyber offensive capabilities is by nations through a process described as the "sovereign cyber effects provided voluntarily by allies."[73] Basically, this approach allows allies to support NATO commanders with cyberattacks, but to keep to themselves (as they choose), the particulars of their offensive cyber methods. Such an approach

[66] While area effect weapons, such as the dual-purpose improved conventional munition (DPICM), remain controversial for most NATO nations, the war in Ukraine has demonstrated their efficacy. NATO nations should consider including DPICMs in their munitions stocks, as they are an effective weapon for SEAD and beyond. While JASSM and TLAM are not the optimal munitions for SEAD, including them in exercises provides additional options for planners to create dilemmas for a defending force.

[67] Franz-Stefan Gady and Alexander Stronell, "Cyber Capabilities and Multi-domain Operations in Future High-intensity Warfare in 2030," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), December 8, 2020, 156, https://ccdcoe.org/uploads/2020/12/8-Cyber-Capabilities-and-Multi-Domain-Operations-in-Future-High-Intensity-Warfare-in-2030_ebook.pdf.

[68] Gady and Stronell, "Cyber Capabilities."

[69] Gady and Stronell, "Cyber Capabilities," 156-157.

[70] Max Lesser, Simon Fellows, and Oakley Cox, "Defending Operational Technology (OT) in Kinetic, Cyber, and Hybrid Warfare," Darktrace Federal, as noted in Industrial Control Systems Working Group quarterly newsletter, US Cybersecurity and Infrastructure Security Agency, June 2022, 3, https://www.cisa.gov/sites/default/files/ICSJWG-Archive/QNL_JUN_2022/Defending%20OT%20in%20Kinetic%20Cyber%20and%20Hybrid%20Warfare_s508c.pdf.

[71] Attacks on civilian infrastructures that are supporting military activities would need to be evaluated in terms of the requirements of the laws of war of military necessity, distinction, and proportionality. See *Department of Defense Law of War Manual*, US DOD, December 2016, 50-65, https://DOD.defense.gov/Portals/1/Documents/pubs/DOD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf.

[72] "Cyber Defence," NATO, August 3, 2023, https://www.nato.int/cps/en/natohq/topics_78170.htm.

[73] Wiesław Goździewicz, "Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)," *Cyber Defense Magazine*, November 11, 2019, https://www.cyberdefensemagazine.com/sovereign-cyber/.

is understandable for security reasons, particularly prior to conflict, as the capacity to breach the cyber defenses of an adversary often relies on sensitive intelligence and methods. However, in conditions of conflict, the value of wartime cyber offensive operations may benefit from broader coordination with kinetic operations.

The discussion below recommends, as part of wartime NATO operations, the establishment and utilization of multidomain task forces that are designed to coordinate effects from all domains including cyber. Precisely how those MDTFs will operate is still to be determined, but if multidomain operations are to be successful, cyber offense will need to be effectively integrated.

2. Cyber defense of key critical infrastructures: In the event of conflict, cyber defense of key critical infrastructures necessary for military operations will rely in significant part on a different type of multidomain activity, namely on partnerships between governments and the private sector, with the latter undertaking operational activities as those now ongoing in Ukraine. Such government-private sector relationships essentially are creating a "sixth domain" in which the operational and coordinated activities of the private sector with government are a sphere of activities in the same sense as the other domains of air, sea, land, cyber, and space.[74] Obviously, private-sector support to militarily critical infrastructures will be key to effective battlefield and logistical operations by NATO forces in the context of a high-intensity conflict with Russia, as is reflected in the discussion above concerning Ukraine.

NATO has recognized the important role of the private sector for cyber defense, but thus far NATO has limited interactions with private-sector cyber defenders to strengthen engagement "through information-sharing, exercises, and training and education."[75] Such activities are, of course, valuable but far from the operational coordination between governments and the private sector that is now taking place in Ukraine. In order to accomplish the degree of cyber resilience that will be required in wartime, NATO member nations will need to have highly capable cybersecurity support from the private sector, as one of the authors noted in an earlier Atlantic Council brief. Specifically, that cybersecurity support is essential "for those critical infrastructure necessary for effective military operations—which will generally involve the electric grid, pipelines, air, rail, and ports, as well as the information and communications networks themselves.[76]

Accordingly, NATO should expand the current cyber requirements established by the Defense Planning Process to generate the appropriate taskings focused on the operational engagement in wartime with the private sector that nations will need to put in place.[77]

D. Dynamic Sustainment

NATO planners and logisticians are well aware of the issues that the United States and other NATO nations will have in promptly building forces in theater and in sustaining those forces to support a fight against Russia. The importance of doing so has been underscored by Russia's disastrous sustainment failure at the outset of its February 2022 invasion of Ukraine.

Planners have long discussed the imperative to have dispersed, resilient logistics infrastructure to evade adversary sensors and to survive long-range strikes. However, what is less discussed is the importance of ensuring that NATO forces have the logistical wherewithal to leverage such dispersed capabilities, including the ability to offset the consequences of degraded civilian critical infrastructures—such as railroads, bridges, pipelines, and electrical capacity—that will be necessary to sustain a fight under realistic combat conditions.

The war in Ukraine provides many lessons for how a large-scale fight may play out. When artillery strikes utilizing longer-range HIMARS weapons forced Russia to move its sustainment operations further from the front lines (and to utilize trucks for dispersion rather than rail lines), their operations were slowed significantly. The key point for NATO is that dispersed, resilient logistics are critical, but the dispersion complicates sustainers' ability to get matériel to the right place at the right time. A successful MDO fight will need to find ways to overcome these challenges.

From a sustainment perspective, it is clear from the war in Ukraine that sustainment will be incredibly important, and that the resource intensity of large-scale combat operations will necessitate a massive logistical lift. What Ukraine is not a good case study for, however, is sustainment operations in the rear. That is because Ukraine has had the benefit of an untouchable rear logistic support area in NATO. If NATO is in conflict, no logistics area—in theater or out, military or civilian—can be considered a safe haven, and NATO logisticians will need to be able to dynamically change sourcing solutions including air, ground, and sea lines of communication (LOCs).

AI capabilities should be developed that can support the requirement to provide dynamic rerouting options when LOCs become unusable. Data proliferation in future conflicts, result-

[74] The "sixth domain" as an operational domain of warfare is discussed in two works by Franklin D. Kramer: *The Sixth Domain: The Role of the Private Sector in Warfare*, Atlantic Council, October 4, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/; and "NATO Deterrence and Defense: Military Priorities," 6-8

[75] "Cyber Defence," NATO.

[76] Kramer, "NATO Deterrence and Defense," 7.

[77] NATO should also coordinate with the European Union to ensure consistency between NATO requirements and the EU's recent network and information security (NIS2) directive with which EU nations are required to comply by October 2024. See "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union," *Official Journal of the European Union*, December 27, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&qid=1672747885309&from=EN.

ing from an increase in available sensors and digital information, will provide challenges and opportunities for logisticians, but AI built and trained for such complexity should be able to provide significant benefits and advise on the most valuable logistical routes and other requirements. By way of example, a Modern War Institute piece notes that the United States is already pursuing "non-commercially dependent distributed logistics" including over the shore "when existing facilities are limited or unavailable—[to be] able to load and unload ships outside of fixed ports."[78] But precisely where such activities should most effectively take place in a wartime scenario could be enhanced by analysis utilizing AI.

At the NATO level, the Joint Support and Enabling Command (JSEC),[79] which falls under the Supreme Allied Commander Europe at SHAPE, is responsible for coordinating sustainment during crisis or conflict. JSEC is leveraging large-scale NATO exercises to gather data about sustainment operations and to build out its reinforcement and sustainment network (RSN), which informs how JSEC advises SACEUR on sustainment.[80] However, JSEC's roles, responsibilities, and authorities have still not been clearly delineated. As NATO works to define and clarify JSEC's role, it should task JSEC with building out its RSN. In a dynamic MDO fight, this capability will be crucial to flowing forces in theater and also to consolidating and building upon gains.

JSEC will also need to work closely with the private sector. As previously noted, private-sector critical infrastructure will be at risk both from kinetic and cyber intrusions, and one critical aspect of multidomain operations will be working with the private sector on cyber security and resilience of critical private-sector infrastructure upon which military operations and basing infrastructure depend. NATO members' national armament directors already have begun to work more closely with industry on munitions stockpiles as a result of Russia's invasion of Ukraine. NATO should use this cooperation as a stepping stone to work more closely with industry on other key tenets of military operational and basing security and resilience. For example, NATO could audit regional private infrastructure risk and establish both regionally focused and NATO-wide critical infrastructure wartime planning councils "with government and private-sector membership . . . to oversee planning for, and coordination of, government and private-sector wartime activities."[81] The military also must have tactics, techniques, and procedures (TTPs) in place to adapt and overcome challenges when relying on private-sector logistics or civilian infrastructure that is degraded or destroyed. NATO should task JSEC to establish such TTPs, including the development of AI capabilities, which will allow for effective alternatives in light of destruction from adversary attack.[82]

E. Survivability and Lethality of Forward-Stationed Forces

US Army doctrine recognizes that friendly forces likely will be isolated and under attack during the initial phases of a conflict. As a result, it lists "survivability and protection of forward-stationed forces when isolated or outnumbered" as one of the key MDO challenges.

Such a scenario could arise in a conflict in which Russia attacks or invades a NATO nation, particularly where Russia or Belarus border NATO countries. NATO planning needs to take account of such a prospect for the geographic area from Finland through Poland and especially for the geographically challenged Baltic states. Each country does have national forces, with Poland and Finland having significant capabilities. Moreover, since Russia's second invasion of Ukraine, the United States has augmented its forces in Europe, including maintaining an armored brigade combat team (BCT) in Poland and a rotational BCT in Romania.[83] Additionally, there are multinational battalions and brigade headquarters in the Baltic countries and Poland. While the aggregate is substantial, it still falls short of the NATO Force Model objective, which states that NATO will have "well over 100,000 Tier 1 forces" within ten days.[84] While the new regional plans are presumably built with this capability in mind, mobility could present challenges to achieving the full force in the time desired and, accordingly, it is possible that NATO forward forces would be outnumbered until the planned forces arrive. As a result, it is important that the national and forward-stationed forces have the capabilities and support necessary to fight a successful defensive action while awaiting reinforcement. Effective use of multidomain operations will help achieve that result.

First, it will be very important for the forward forces to be heavily supported by large quantities of standoff weapons, including long-range fires, air-ground munitions, land-based anti-air capabilities, land-based anti-ship missiles, and cluster munitions

[78] Garrett Chandler and Matthew Carstensen, "Lots to Be Desired: Why the US Army Needs to Invest in Logistics Over-the-Shore," Modern War Institute, April 28, 2022, https://mwi.westpoint.edu/lots-to-be-desired-why-the-us-army-needs-to-invest-in-logistics-over-the-shore/.

[79] JSEC was established in 2018 and just reached full operational capability in 2021.

[80] The Reinforcement and Sustainment Network (RSN) is a JSEC-created database of sustainment-related physical infrastructure assets throughout NATO's area of operations and the laws, regulations, and other administrative factors that impact the infrastructure's utilization and maintenance. See "Exercise Spring Storm in Estonia—and the Link to JSEC in Ulm, Germany," NATO news release, May 26, 2023, https://jsec.nato.int/newsroom/news-releases/exercise-spring-storm-in-estonia-and-the-link-to-jsec-in-ulm--germany-2.

[81] Kramer, *The Sixth Domain*, 4.

[82] *Agile Combat Employment*, US Air Force, August 23, 2022, 5-7, 9, 11, https://www.doctrine.af.mil/Portals/61/documents/AFDN_1-21/AFDN%201-21%20ACE.pdf. NATO will also need to utilize resilience techniques such as, in the case of aircraft, hardened shelters, assuring sufficient fuel at contingency bases, and undertaking deception techniques such as camouflage.

[83] "Fact Sheet—U.S. Defense Contributions to Europe," US DOD, June 29, 2022, https://www.defense.gov/News/Releases/Release/Article/3078056/fact-sheet-us-defense-contributions-to-europe/.

[84] "New NATO Force Model," NATO, 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-infographic-newnato-force-model.pdf.

to halt a Russian advance.[85] As should be obvious, multidomain ISR capabilities would support both the forward forces and those supporting them.

Second, unmanned systems are absolutely crucial for a smaller, defending force. This is why frontline nations should invest heavily in large quantities of unmanned aerial systems (and depending on their location, unmanned maritime systems as well). The obvious corollary to this recommendation is that frontline forces will themselves be susceptible to detection and attack emanating from low-cost, unmanned systems. As the war in Ukraine demonstrates, both sides have struggled to stay on the winning side of the value proposition in countering unmanned aerial systems (UAS), often forced to use high-value or low-density assets to counter cheap drones. NATO and its constituent countries should therefore cooperate in the development of cheap, reliable counter-UAS technologies that leverage kinetic and nonkinetic means. Given the nature and scope of this technological race, counter-UAS technologies could be an important area of focus for the recently established Defence Innovation Accelerator for the North Atlantic (DIANA), which provides mentoring and grant financing to start-ups developing technologies that can answer key "challenges" that face NATO militaries.[86]

Third, frontline forces—and the militaries of the nations in which they are stationed—should be structured in a way that allows for disaggregated, smaller-unit operations and equipped with platforms that provide asymmetric spoiling capabilities. To the extent possible, those forces also should be capable of pairing with and augmenting the high-end capabilities that follow-on forces will employ across domains as part of a counterattack.

A primary example of this type of capability that requires geographic proximity, can be operated by small teams, and can create opportunities for employment of high-end capabilities are the electronic warfare (EW) hunting teams that Ukraine is employing in its fight against Russia. These small, covert teams range the battlefield to detect electronic signatures from Russian weapons systems and then provide coordinates to friendly units able to target the systems. In an MDO scenario, a high-end capability from the land, air, or maritime domain may be the platform that ends up taking the shot based on information from the hunt team. As discussed above, Ukraine has developed several such systems, and NATO should determine whether to utilize them or to develop comparable capabilities.[87] In order for this high-low mix to work, a survivable, secure communications system will be absolutely essential. This is another key capability that frontline countries should invest in for an MDO fight.

F. Space

NATO has recognized space as a key element of multidomain operations. At the 2023 Vilnius summit, allies stated: "As part of our work on space as an operational domain, we are accelerating the integration of space into planning, exercising and executing joint and multi-domain operations in peacetime, crisis, and conflict in order to ensure space effects are coordinated across all domains."[88]

The Vilnius communique noted the establishment of NATO's Alliance Persistent Surveillance from Space (APSS) multinational program, "which will improve NATO's intelligence, surveillance and reconnaissance capacity."[89] The APSS initiative—called multiyear, multidomain, and multinational—is designed to achieve both "persistent surveillance" and the "speed at which space-based data is collected, aggregated and delivered," aimed at making "more effective use of both government-owned and commercial space-based assets."[90]

The vision is further described by NATO:

> APSS is not about creating NATO-owned and operated space assets. It will make use of existing and future space assets in Allied countries, and connect them together in a NATO virtual constellation called "Aquila." This is a data-centric initiative. As such, APSS will be "sensor-agnostic and solution-agnostic"; it will be open to all existing—and future—space assets, regardless of their scope, technologies and specificities. It will bring together both government-owned and commercial space assets.[91]

In addition to APSS, NATO had previously undertaken to engage with national space capabilities through the establishment of the NATO Space Centre, which "serves as a focal point to support NATO's activities, operations and missions; share information; and help coordinate Allies' efforts in the space domain, [including] reach[ing] out to national space entities to ensure that NATO commanders have access to required space data and services."[92]

[85] As demonstrated in Ukraine and planned for in Korea, cluster munitions capabilities such as DPICMS and rapidly deployable mine systems such as the family of artillery-scatterable mines (FASCAM) are key elements of defense in a high-intensity conflict.

[86] DIANA is a new initiative, and 2023 is its pilot year. It seeks to help solve key military "challenges" by mentoring and providing grant financing to technology start-ups to get them through the "valley of death" of technological innovation. For 2023, the three challenges DIANA sought proposals for all have MDO applications; they are undersea sensing, energy resilience, and secure communications. While counter-UAS is not currently one of the three key challenges that DIANA is focused on solving, it should be considered for inclusion in DIANA's Strategic Directive for the next two years, which is currently being written.

[87] Frontline forces can also make the enemy's job more difficult by utilizing systems that emit fake electronic signatures to draw enemy fires from high-value targets and use AI-enabled cyber campaigns to flood the publicly available information (PAI) space and degrade an enemy's ability to use PAI for targeting.

[88] Vilnius Summit Communiqué, NATO press release, July 11, 2023, paragraph 67, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

[89] Vilnius Summit Communiqué, NATO. The communique also referenced the "establishment of the NATO Space Centre of Excellence in France."

[90] "Alliance Persistent Surveillance from Space (APSS)," NATO, February 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230215-factsheet-apss.pdf

[91] "Alliance Persistent Surveillance from Space (APSS)," NATO.

[92] "NATO's Approach to Space," NATO, May 23, 2023, https://www.nato.int/cps/en/natohq/topics_175419.htm.

Further illustrating NATO's recognition of space's inherent multidomain nature is provided by NATO's Coalition Warrior Interoperability Exercise (CWIX), which NATO describes as its "Premier Interoperability Exercise."[93] CWIX 2023 included a focus on space as part of meeting the Alliance's MDO ambitions, with the aim of integrating it as an operational domain.[94]

As the foregoing suggests, NATO's reliance on both governmental and commercial satellites means that it will undertake to make extensive use of the proliferation of LEO satellites. In wartime, that will significantly add to the resilience of the NATO space enterprise. A Mitchell Institute paper describes the impact on deterrence:

> The use of small, inexpensive satellites in a [proliferated low-earth orbit] constellation also improves deterrence because of its increased cost imposition potential. The cost of a direct-ascent kinetic antisatellite is now greater than the target satellite, and because of the sheer number of assets an enemy must attack, proliferation reduces the effectiveness and impact of these weapons and other coorbital threats.[95]

In light of NATO's developing space architecture that includes reliance on commercial space capabilities, a key issue for wartime will be to ensure that the commercial capabilities being relied upon are in fact available for use as required. Inasmuch as satellites are national assets, arrangements to assure availability will have to be established at the national level. One model for such assurance that deserves review would be based on ongoing actions by the United States.

Currently, the United States is undertaking to establish contractual arrangements with satellite companies somewhat along the lines of those utilized by DOD for support from the airline and maritime industries. By way of background, the civil reserve air fleet (CRAF) provides "selected aircraft from U.S. airlines [which are] contractually committed to CRAF [to] augment Department of Defense airlift requirements in emergencies when the need for airlift exceeds the capability of military aircraft."[96]

The US Space Force is now in the process of developing a commercial augmentation space reserve (CASR) program. As with CRAF, CASR would seek to establish "voluntary pre-negotiated contractual arrangements" that would provide support to the military by ensuring that "services like satellite communication and remote sensing are prioritized for US government use during national security emergencies."[97]

While each NATO nation with space capabilities will need to determine its own national framework, the CASR program offers a useful starting point. Among the issues that would need to be considered are which services, and in what amounts, could reliably be provided in a wartime environment; whether such services could be based on existing (or planned) private-sector constellations or whether those would need to be expanded; what provisions would need to be made for satellite and/or ground station replacement in the event of adversary attacks; what provision for indemnification would need to be agreed upon; and what level of funding would be appropriate both to incentivize the private sector, accomplish the requisite wartime tasks, and undertake planning and training prior to conflict.

It is worth pointing out—especially in light of the noted limitation placed on Ukraine's use of Starlink—that the US Defense Production Act, if necessary, authorizes the government to require the prioritized provision of services—which would include services from space companies—and exempts any company receiving such an order from liabilities such as inability to support other customers.[98] It would, of course, be much more desirable and effective if the arrangements were established in advance through a voluntary program, as the CASR program is seeking. However, other NATO nations will need to determine if they have or would want comparable mandatory authorities.

G. Command and Control Structures for MDO

NATO has just approved its new regional plans. Their implementation will almost certainly require revision of the command arrangements that heretofore have been built around the concept of a 40,000-person NATO Response Force, largely focused on out-of-area missions. By contrast, as noted above, the new NATO Force Model is intended as a European-focused force designed to meet the Russia military challenge by providing "well over 100,000 Tier 1 forces" within ten days and about "200,000 Tier 2 forces" in about ten to thirty days.[99] How multidomain operations will fit into these new approaches is as yet less than clear.

As an initial matter, however, it seems likely that operationalizing MDO will require—along the lines set forth by the unclassified summary of the DOD JADC2 strategy—"reforming, realigning, or creating organizations with the structure, agility, and resources to more effectively blend physical and informa-

[93] "Allied Command Transformation Leads the Execution of the Annual Coalition Warrior Interoperability Exercise," NATO ACT, June 5, 2023, https://www.act.nato.int/article/act-leads-2023-cwix/.

[94] "Allied Command Transformation Leads the Execution," NATO ACT.

[95] Charles S. Galbreath, "Building U.S. Space Force Counterspace Capabilities: An Imperative for America's Defense," Mitchell Institute, June 2023, 16, https://mitchellaerospacepower.org/wp-content/uploads/2023/06/Building-US-Space-Force-Counterspace-Capabilities-FINAL2.pdf.

[96] "Civil Reserve Air Fleet," US Air Force, accessed July 4, 2023, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104583/civil-reserve-air-fleet/.

[97] Sandra Erwin, "Space Force to Further Define Details of a 'Commercial Space Reserve,' " *Space News*, July 25, 2023, https://spacenews.com/space-force-to-further-define-details-of-a-commercial-space-reserve/#:~:text=Open%20dropdown%20menu,Space%20Force%20to%20further%20define%20details%20of%20a%20'commercial%20space,Sandra%20Erwin%20July%2025%2C%202023.

[98] US Defense Production Act of 1950, 50 U.S.C., §§ 4511, 4557.

[99] "New NATO Force Model," NATO, 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-infographic-newnato-force-model.pdf.

tional power of the joint force and its mission partners."[100] To be sure, given the still emerging contours of NATO command and control planning, organizational restructuring to effectuate MDO will be less than immediate—and that is particularly true since the United States is itself very much still in development with respect to MDO.[101]

There is, however, one effort that NATO could undertake for such "reforming, realigning, or creating organizations" for MDO consistent with ongoing actions by the United States. NATO should incorporate as part of its wartime planning the "multidomain task forces" in the process of being created by the US Army to include the activated 2nd Multi-Domain Task Force in the US European Command (EUCOM). The MDTF recently completed an exercise undertaken to "validat[e] the progress of modernization efforts of continuous integration of effects in various domains, including air, land, sea, space, and cyberspace."[102] As a subsequent related step, NATO could undertake to establish comparable combined task forces for the broader NATO force.

The creation of US Army multidomain task forces is part of a significant reorganization that the Army is undertaking to enhance its capability to prevail in high-intensity battle. That effort importantly focuses on MDO. As described by Gen. James Rainey and Lt. Gen. Laura Potter:

> Last fall, the Army published Field Manual 3-0, *Operations*, transitioning multidomain operations from concept to doctrine. . . . Multidomain operations require commanders to synchronize effects from land, air, sea, space, and cyber to defeat an adversary in concert with our allies and partners as part of the joint force.[103]

Accordingly, the Army is moving significant operational control to "higher echelons of theater army, corps, and divisions," and building new organizational capabilities including the "joint task force-certified Army corps."[104] The corps has critical MDO functions:

> Corps are the Army's primary echelon for synchronizing and delivering multidomain effects. A corps staff must synthesize the vast amount of data received from land, air, the electronic spectrum, and space sensors to create a shared visualization of the complex battlefield and then set conditions for divisions to dominate the close fight. Corps commanders bear responsibility for shaping the deep battle by synchronizing the delivery of long-range fires like missiles, aircraft, and unmanned vehicles with cyber, space, or information operations to disrupt an adversary's operational level of operations.[105]

In conjunction with this overall realignment, Army multidomain task forces are designed to support the synchronization and integration of MDO operations undertaken by higher echelons:

> Multidomain task forces are purpose-built formations capable of coordinating and integrating cyberspace, electromagnetic activities, and space capabilities with long-range surface fires to deny enemy commanders the ability to prohibit friendly forces from operating in any land, air, or sea area.[106]

In the near and medium term, NATO should undertake efforts comparable to those being undertaken by the US Army. As NATO's new regional plans are put into place, NATO should establish for its ground forces the same theater-corps-division construct that the US Army is establishing. Multidomain task forces likewise will be needed to coordinate the capabilities available from all domains. Starting NATO's implementation of MDO with US Army MDTFs will provide a practical basis for effectuating NATO MDO that can rely on US lessons learned and on the US Army as an MDO backbone.

III. A MULTITIERED APPROACH TO MDO

The time to move forward with implementation of MDO is now. To do so, NATO should adopt a multitiered approach that plays to the relative strengths inherent in different nations due to geography and economics.

In undertaking to establish MDO capabilities within the NATO force structure, it is important to take a realistic approach to the economic issues surrounding defense budgets, especially given requirements arising as a consequence of the Ukraine-Russia war. Multiple European economies are under strain as a re-

[100] *Summary of the Joint All-Domain Command & Control (JADC2) Strategy*, DOD, 6.

[101] To be sure, significant efforts focused on capabilities are being undertaken by the Department of Defense. These include the Air Force's Advanced Battle Management System, the Army's Project Convergence, and the Navy's Project Overmatch, as well as activities by the Chief Digital and Artificial Intelligence Office in the Office of the Secretary of Defense. However, as noted, those activities are as yet developmental, and, illustratively, as described in a January 2023 report by the Government Accountability Office focused on the US Air Force: the "Air Force has not delivered any capabilities to date." See *Battle Management: DOD and Air Force Continue to Define Joint Command and Control Efforts*, Government Accountability Office, January 2023, highlights (unnumbered first page), 7, https://www.gao.gov/assets/820/814635.pdf; and *Defense in a Digital Era Hearing Before the House Armed Services Subcomm. on Cyber, Information Technology, and Innovation*, 118th Cong. (2023) (statement for the record of Dr. Craig Martell, DOD chief digital and artificial intelligence officer), https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/Martell%20Testimony.pdf.

[102] Maj. Jacqwayne Griffin, "The Army's Future Fight: Maximizing 2nd Multi-domain Task Force's Unprecedented Arcane Thunder 23 Exercise," US Army, September 7, 2023, https://www.army.mil/article/269715/the_armys_future_fight_maximizing_2nd_multi_domain_task_forces_unprecedented_arcane_thunder_23_exercise.

[103] *Summary of the Joint All-Domain Command & Control (JADC2) Strategy*, DOD, 6.

[104] *Summary of the Joint All-Domain Command & Control (JADC2) Strategy*, DOD, 6.

[105] *Summary of the Joint All-Domain Command & Control (JADC2) Strategy*, DOD, 6.

[106] *Summary of the Joint All-Domain Command & Control (JADC2) Strategy*, DOD, 6.

sult of the increased cost of energy following Russia's invasion of Ukraine, outlays of support to the Ukrainian Armed Forces, support to refugees and other humanitarian and economic assistance for Ukraine, and the flood of Ukrainian foodstuffs into Europe as a result of Russia's withdrawal from the Black Sea grain deal—all the while still dealing with the COVID-19 pandemic's hit to their economies. While all NATO nations have agreed to spending 2 percent of gross domestic product as a floor for their defense budgets, how that is spent will be quite important as nations evaluate multiple requirements, including the expenditures needed in order to backfill equipment donated to Ukraine, refill depleted munitions stockpiles, invest in new capabilities and platforms, and scale capabilities for high-intensity conflict.

In the context of MDO, a multitiered approach will both help accommodate economic constraints while nonetheless generating highly effective capabilities. Most specifically, it is important to underscore that not all NATO nations will need all key capabilities. Smaller countries should not chase after high-end, expensive capabilities such as those that can have effects at standoff distances, but rather should look to low-cost, highly effective attritable capabilities like those described in the Replicator initiative. Frontline countries should also include capabilities that require geographic proximity for employment and can be employed by smaller, dispersed units. Larger nations, however, can undertake to acquire capabilities that require expensive platforms. As the Replicator initiative implies, a high-low mix will be warranted for maximum effectiveness.

The mix of platforms that larger and smaller countries pursue should not just be interoperable. They should be mutually reinforcing when employed in concert. Using SEAD as an example:

> No NATO nation aside from the United States could conduct a SEAD campaign, but all NATO nations, and especially frontline NATO nations, should consider how the capabilities they pursue and adopt could support portions of the F2T2EA process. For example, smaller nations could invest in sensing, cyber, and [special operations forces] capabilities to support the find, fix, target, track, and assess portions of SEAD, while larger nations can invest in fifth generation aircraft and long-range fires capabilities to assist with the engage portion of the process.

Three key factors should drive what platforms NATO countries acquire. First, nations should look to what the United States is acquiring and developing in support of an MDO fight. This is because the United States is further ahead than any other NATO nation on MDO, so NATO and its constituent nations should build around US progress.

Second, NATO and its constituent nations should be informed by the five-step NATO Defense Planning Process (NDPP) and heavily influenced by the three regionally focused defense plans. In Vilnius, NATO completed step one of the NDPP—establish political guidance—when it approved the Political Guidance for Defence Planning 2023 and its three regionally focused defense plans. Now NATO must execute the remaining NDPP steps: determine requirements, apportion requirements, facilitate implementation, and review results.

This report has recommended seven potential capability areas for near-term focus during the requirements determination process, which will establish minimum capability requirements for the Alliance. NATO's Allied Command Transformation and Allied Command Operations strategic commands lead steps two and three, and while both steps are important, in a budget-constrained environment, the third step of the process—when ACT and ACO apportion out the minimum capability requirements as capability target packages for individual nations or groups of nations—will be absolutely critical to successful adoption of MDO. ACT and ACO will have to take a strategic view of how to deconflict acquisitions and coordinate training and collective capability development in an iterative manner. NATO should identify capabilities that require mass or significant quantities, and ensure that acquisition mechanisms are coordinated to achieve mass. MDO needs communication and timing across domains to work. Coordinating this across five domains and thirty-one (hopefully soon to be thirty-two) nations is a huge undertaking requiring significant doctrine and training. The Alliance should focus on leveraging the NATO Defense Planning Process as a vehicle to harmonize national and Alliance processes in a way that meets NATO's warfighting objectives.

Third, countries should ensure that testing and experimentation inform their acquisitions process. Rather than trying to plan out a 90 percent solution before a single acquisition is made, countries should iterate and exercise capabilities in simulated combat settings to inform what they eventually adopt. This is precisely the approach that the US Army is pursuing with its Project Convergence. It seeks to repeatedly get technologies into the hands of its soldiers to test them in combat environments and see not only what technologies work, but also how soldiers are able to leverage technologies in novel ways. While this would not lead to all NATO nations marching in unison, it would at least help all nations walk in the same direction. Given the speed of technological innovation, this iterative approach would benefit the Alliance as a whole not just by allowing for continuous adoption of newer technologies, but also by having technology adoption be better tied to warfighting needs based on tactical and operational experimentation. For example, NATO nations should exercise capabilities like the GIS Arta system in a multilateral, multidomain environment to see what impact it has on the battlespace.

IV. CONCLUSION: TOWARD COMBINED-ALL DOMAIN OPERATIONS

As the war in Ukraine has demonstrated, NATO's ability to set the pace—and ultimately dominate—in the future battlespace will require the accelerated modernization of its digital infrastructure and mastery of synchronized activities across all domains and threat environments. To realize its vision for an MDO-enabled Alliance, NATO must move beyond efforts to align at the conceptual level by prioritizing the adoption and integration of capabilities that enhance its defense and deterrence posture across domains. Near- and medium-term capabilities such as sensor-shooter networks, AI-enabled agile logistics, private-sector space assets, and others outlined in this brief will accelerate the ability of NATO allies large and small to execute combined all-domain operations with agility and in unison—ensuring the advantage remains tilted in favor of the transatlantic community and the democratic values that define it.

ABOUT THE AUTHORS

Franklin D. Kramer is a distinguished fellow and board director at the Atlantic Council. Kramer has served as a senior political appointee in two administrations, including as assistant secretary of defense for international security affairs. At the Department of Defense, Kramer was in charge of the formulation and implementation of international defense and political-military policy, with worldwide responsibilities including NATO and Europe, the Middle East, Asia, Africa, and Latin America.

In the nonprofit world, Kramer has been a senior fellow at CNA; chairman of the board of the World Affairs Council of Washington, DC; a distinguished research fellow at the Center for Technology and National Security Policy of the National Defense University; and an adjunct professor at the Elliott School of International Affairs of The George Washington University. Kramer's areas of focus include defense, both conventional and hybrid; NATO and Russia; China, including managing competition, military power, economics and security, and China-Taiwan-US relations; cyber, including resilience and international issues; innovation and national security; and irregular conflict and counterinsurgency.

Kramer has written extensively. In addition to the current issue brief, recent publications include *The Sixth Domain: the Role of the Private Sector in Warfare; NATO Deterrence and Defense: Military Priorities for the Vilnius Summit*; *NATO Priorities: Initial Lessons from the Russia-Ukraine War*; *China and the New Globalization*; *Free but Secure Trade*; "Here's the 'Concrete' Path for Ukraine to Join NATO"; and *Providing Long-Term Security for Ukraine: NATO Membership and Other Security Options*.

Ann M. Dailey is a nonresident senior fellow at the Transatlantic Security Initiative of the Atlantic Council's Scowcroft Center for Strategy and Security and is currently serving as a policy researcher at the RAND Corporation; however, the views, opinions, findings, conclusions, and recommendations contained herein are the author's alone and not those of RAND/or its research sponsors, clients, or grantors.

Dailey is a geopolitical strategist with deep expertise in Europe, Eurasia, and energy and climate resilience with two decades of study and experience in the public and private sectors. She is a former senior adviser to the assistant secretary of defense for international security affairs in the Office of the Under Secretary of Defense for Policy, and previously served as senior adviser for Russia, Ukraine, and Eurasia in the Office of the Undersecretary of Defense. She has a master of arts in international economics from the Johns Hopkins School of Advanced International Studies and a bachelor of arts in political science, international studies, and Russian and Eurasian studies from the University of Illinois. Dailey is also an engineer captain in the US Army Reserve.

Joslyn A. Brodfuehrer is an assistant director with the Transatlantic Security Initiative (TSI) at the Atlantic Council's Scowcroft Center for Strategy and Security. In this capacity, she supports TSI's efforts to strengthen the transatlantic alliance against emerging security threats. She previously served as a program assistant at the National Endowment for Democracy's International Forum for Democratic Studies, where she supported the center's information space and emerging technologies research portfolios. Prior to joining the International Forum, Brodfuehrer held internships at the US Department of State (the US embassy in Costa Rica) and the Office of the US Trade Representative (the World Trade Organization and Multilateral Affairs Office).

Brodfuehrer holds a master of philosophy in politics and international studies from the University of Cambridge. She graduated summa cum laude from Lafayette College with a bachelor of arts in international affairs and government and law, focusing on global conflict and cooperation.

ACKNOWLEDGMENTS

Lt. Col. Tyson K. Wetzel, a nonresident senior fellow in the *Forward* Defense practice of the Atlantic Council's Scowcroft Center for Strategy and Security, and **Conor Rodihan**, a former associate director in the Scowcroft Center for Strategy and Security's Transatlantic Security Initiative, made critical contributions in the early stages of the report's conceptualization.

Atlantic Council

Board of Directors

**Executive Committee Members*

List as of July 5, 2023

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org