GLOBSEC
IDEAS SHAPING THE WORLD

Connect to Succeed: Multi-Domain Operations Readiness on the Eastern Flank

GLOBSEC Future Security and Defence Council

Final Version

www.globsec.org

CREDITS

GLOBSEC

Vajnorská 100/B
831 04 Bratislava
Slovakia

www.globsec.org

GLOBSEC is a global think-tank based in Bratislava committed to enhancing security, prosperity and sustainability in Europe and throughout the world. Its mission is to influence the future by generating new ideas and solutions for a better and safer world. We believe we can change the world by putting together the right stakeholders at the right time for a free exchange of ideas. In an interconnected world, GLOBSEC stimulates public-private dialogue to shape agendas for the future. With global ambitions in mind and building on its Central European legacy, GLOBSEC seeks to contribute to agendas that are critical for Europe. GLOBSEC acts in the spirit of European values and international cooperation.

FUTURE SECURITY & DEFENCE COUNCIL

The GLOBSEC Future Security & Defence Council is an initiative supported by an Advisory Committee made up of renowned defence experts, national and private sector leaders, and champions of international diplomacy. It is designed to connect a diverse set of public and private stakeholders and act as a centre for idea generation and exchange that will deliver pragmatic policies and strategies. The process includes regular meetings of the Council and consultations

AUTHORS

Lead Writer

Alexander Lanoszka, Associate Professor,Department of Political Science, University of Waterloo

Content Editor

Marcin Zaborowski, Senior Policy Fellow, Defence and Security Stream at GLOBSEC

DISCLAIMER

The publication of the report does not imply that all FSDC members endorse the content and recommendations it contains.

DATE

August 2024

GLOBSEC
IDEAS SHAPING THE WORLD

"Multi-Domain Operations is much more than command and control."

Gen. (Ret.) Philip M. Breedlove,
Former Supreme Allied Commander Europe (SACEUR) of NATO Command Allied Operations

Executive Summary

Multi-Domain Operations (MDO) have received wide attention across the North Atlantic Treaty Organisation (NATO), with multiple national militaries embracing the concept and fitting it to their circumstances. NATO's own two strategic commands have conceptualised MDO in an alliance document published in 2023. MDO will thus inform how militaries in the Euro-Atlantic will acquire and incorporate capabilities in the foreseeable future.

Yet the process of this transformation remains in its early stages. As a doctrine, MDO has attracted concern from its initial conception to its potential implementation. Within NATO itself, members vary widely in how they regard specific elements of MDO as well as in the attention that they even give to the concept. Many writings on the subject concentrate largely on the United States and its Western European allies to the neglect of the so-called eastern flank—those easternmost countries stretching from the Baltic Sea to the Black Sea, from Finland to Bulgaria. Unfortunately, any military conflict in Europe where MDO concepts will find their application will almost certainly involve them. Because those countries have been stepping up their defence investments while Russia continues its full-scale attack on Ukraine, now is the time to evaluate what MDO can do for the region.

The purpose of this report is to contribute to the large and growing literature on MDO by examining its applicability to the eastern flank. After describing its lineage and basic doctrinal ideas, it shows how Russia's military performance has largely validated MDO assessments with regard to Russia's electronic warfare, missile and information and cyber capabilities.

Subsequently, it takes up the following issues. First, to what extent and how do eastern flank militaries articulate and incorporate MDO? The answer here is that they seldom do so explicitly in official documents. Second, are eastern flank militaries at least thinking of connectivity, broadly defined, whether between parts of governments, military units and the platforms themselves? On this question, eastern flank militaries are thinking more and more about connectivity, but not all of them do such systematic consideration of the problem. Third, how should eastern flank countries organise and test their MDO in terms of an operational campaign? Much, of course, depends on a country's specific context. However, Poland and the Baltic countries should align the newly announced Baltic Defence Line and 'Eastern Shield' along MDO principles, given the crucial importance of sensory information and battlespace awareness. In Southeastern Europe, Bulgaria and Romania should note that, in sinking a large portion of the Black Sea Fleet, Ukraine has had to develop and to maintain extensive kill chains that require fusing information across multiple military units and government bodies.

Nine recommendations flow from the analysis of MDO and its application to the eastern flank. These recommendations are expanded in detail in the final portion of the report.

1. **The Alliance Must Ensure a Common Understanding of Multi-Domain Operations:** As MDO has not significantly influenced defence thinking along the eastern flank, NATO has a unique opportunity to promote a shared understanding of this vital concept, harmonising doctrinal differences among older members and addressing the lack of awareness among newer ones.

2. **Multi-Domain Operations Are Much More Than Command and Control:** different branches of the military must work seamlessly together, overcoming service-specific biases and bureaucratic barriers. MDO requires not just the eradication of such barriers, but also the active integration of very different skill sets. MDO requires a deep cultural change so as to overcome inter-service rivalries and other organisational barriers to data management, sharing and employment.

3. **Breaking Service Silos: Military Culture Must Transform:** One vector through which to go about a change of attitude is through professional military education programmes, especially at the general and staff levels. Military education across the region, whether at the Baltic Defence College or in national military academies, should impart MDO values and thinking. On the civilian side, civilian leaders also must contribute to meaningful cultural transformation by promoting organisational practices and norms that encourage inter-service collaboration.

4. **Strengthen the Kill Chain: Prioritise Connectivity to Facilitate Operations:** To address potential confusion surrounding MDO, defence establishments should at the very least think in terms of connectivity. Specifically, they should be concerned with how different platforms—both within and between militaries—can interconnect to enhance the effectiveness of the kill chain.

5. **Connect to Project: Sensor Technology Must Be Integrated Throughout the Baltic Defence Line and Poland's 'Eastern Shield':** Extensive sensor technology must be integrated throughout the fortification networks along Poland and the Baltic countries' eastern frontiers. Data collected by those sensors would need to be linked to various command and control structures as well as to frontline units and their follow-on forces. Moreover, the planned fortifications cannot be pursued in isolation from existing allied efforts. They should help organise how NATO militaries conceive of their theory of victory vis-à-vis Russia in a major land war.

6. **Learn From the "Land Down Under":** Dominate the Skies and Shores: Many eastern flank countries are prioritising air and coastal defence as a result of Russia's full-scale invasion. They should consider Australia's own experience since it has been acquiring those capabilities in a manner aligned with MDO thinking. It began devising a Joint Air Battle Management that integrated ground-based radars for developing a situational awareness of what was happening in and around Australian

air space, and for directing aircraft to specific places at specific times for specific purposes. They began to fill in their air defence so that it would be integrated and thus able to defeat various types of threats. Electronic warfare, ground, and cyber capabilities should complement the system, with guided-missile destroyer-type ships contributing to air defence ships. Eastern flank countries can consider what worked for Australia, and what did not since they are going down a similar path.

7. **Stress-Test the Network: Push Connectivity to its Limits Through Military Exercises:** Scenarios are practical because they help unify participants around a shared understanding of the problem. More pointedly, a military exercise or war game organised around a particular problem can identify instances when friendly units have trouble communicating with one another, cannot share data across domains and units, as well as experience disruption due to EW. Still, defence establishments must overcome their reluctance to conduct rigorous exercises for fear of exposing weaknesses, as identifying and addressing these weaknesses is crucial for improvement. Failure does not negatively affect progress. Indeed, exercising to failure is essential to reveal and address weaknesses.

8. **Mission-Driven Acquisition: Focus Procurement on the Mission, Not the Platform:** Many defence establishments tend to focus their procurement and acquisition efforts on specific platforms. Those platforms may have significant military value, but they also can be expensive, carry with them high opportunity costs, and may not even have enough available personnel who could operate them. There may be no plans to connect those platforms until after they have been acquired. Having a common acquisition group, as Australia does, helps build interoperability because it is focused on the mission (e.g., air defence) rather than on particular platforms, all while avoiding the stove-piping and redundancies that characterize the US military.

9. **Learn From Ukraine: Balance Technological Optimism with Industrial Production:** Ukraine's defence against Russian military aggression remains a vivid, if bitter, reminder that industrial warfare requires significant industrial production. Russia depends on its artillery to make territorial gains. In early 2024, Russia was able to make some advances against Ukraine because it made up for its own shortages by receiving large amounts of ammunition and missiles from Iran and North Korea just when the United States was domestically hamstrung from providing more assistance. MDO is a moot point if under-investment and a lack of production leave countries quickly outgunned and depleted. Connectivity across domains is critical to the effectiveness of any military mission in the contemporary era, but military supplies are of existential importance.

Introduction

In 2018, the US Army released its much-awaited doctrinal concept for Multi-Domain Operations (MDO).[1] By this time, the US Department of Defence was focusing less on the expeditionary operations that characterised the Global War on Terror and more on the national security challenges posed by the People's Republic of China and the Russian Federation.[2] Not least because the US Army plays a pivotal role in European security, and the multifaceted threat that Russia poses to the Euro-Atlantic community, MDO has received wide attention across the North Atlantic Treaty Organisation (NATO), with multiple national militaries embracing the concept and adapting it to their circumstances. NATO's own two strategic commands have conceptualised MDO in an alliance document published in 2023.[3] MDO will thus guide how militaries in the Euro-Atlantic will acquire and incorporate capabilities in the foreseeable future.

Yet the process of this transformation remains in its early stages. As a doctrine, MDO has attracted concern from its initial conception to its potential implementation. Within NATO, members vary widely in their views on specific elements of MDO as well as in the attention they give to the concept. Many writings on the subject concentrate largely on the United States and its Western European allies. Despite their proximity to Russia and the acute need for robust deterrence and defence among them, countries on the so-called eastern flank of the Alliance—from Finland down to Bulgaria—receive much less consideration. These countries are on the front line. Any military conflict in Europe where MDO concepts will find their application will almost certainly involve them. Because those countries have been stepping up their defence investments while Russia continues its full-scale attack on Ukraine, now is the time to evaluate what MDO can do for the region.

The purpose of this report is to fill this gap in the extensive and growing literature on MDO. This report begins with a brief account of the conceptual development of MDO, discussing the various technologies that make it possible as well as the implementation challenges anticipated by military analysts. It then evaluates the threat environment to determine how it has changed since the US Army released its doctrine in 2018. Specifically, it evaluates the threat assessment with special reference to Russia and its performance in its attempted full-scale invasion of Ukraine. After all, MDO is threat-centric—the original basis for MDO is the recognition that China and Russia present a much more challenging problem set to the United States and its allies and partners than the militant organisations that preoccupied defence planners during the Global War on Terror. Russia's military performance has largely validated MDO assessments regarding Russia's electronic warfare, missile, and information and cyber capabilities.

The report then discusses MDO in the context of the eastern flank. In so doing, it takes up three questions. First, to what extent and how do eastern flank militaries articulate and incorporate MDO? The answer here is that they seldom do so explicitly in official documents. Second, how are eastern flank militaries thinking of connectivity, broadly defined, whether between parts of governments, military units, and the platforms themselves? On this question, eastern flank militaries are thinking more and more about connectivity, but not all of them do. Third, how should eastern flank countries organise and test their MDO in terms of an operational campaign? Much, of course, depends on a country's specific context. However, Poland and the Baltic countries should align the newly announced Baltic Defence Line along MDO principles given the crucial importance of sensory information and battlespace awareness. In Southeastern Europe, Bulgaria and Romania should note that, in sinking a large portion of the Black Sea Fleet, Ukraine has had to develop and to maintain extensive kill chains that require fusing information across multiple military units and government bodies. Thereupon the report concludes with nine policy recommendations for practitioners to consider.

1 Headquarters, Training and Doctrine Command (TRADOC), The U.S. Army in Multi-Domain Operations 2028, TRADOC Pamphlet 525-3-1 (Fort Monroe, VA: TRADOC, 2018), **https://www.tradoc.army.mil/Portals/14/Documents/MDO /TP525-3-1_30NOV2018.pdf**.
2 Jim Mattis, Summary of the 2018 National Defense Strategy of the United States: Sharpening the America's Military Competitive Edge (Arlington, VA: US Department of Defence, 2018).
3 Allied Command Transformation, "Ongoing Military Transformation, Leading to NATO 2030 – Multi-Domain Operations, Deterrence and Defence, Improved Understanding," NATO, 23 March 2023, **https://www.act.nato.int/article/ongoing-military-transformation-leading-to-nato-2030-multi-domain-operations-deterrence-and-defence-improved-understanding/**.

1. MDO and the Threat Environment

MDO addresses a basic military-strategic problem: China and Russia have acquired a panoply of capabilities that complicate the ability of the United States, its friends and allies to move their forces into and around particular theatres of operations. Political and territorial control in such areas as the Baltic littoral region or the Western Pacific may become highly contested. The challenge is inherently multi-domain because ground, naval and air units can deploy missiles and fire long-range weapons at targets identified and processed more speedily thanks to greater computing power and network connectivity.

This problem set differs from what was typical of the Western military experience after 1991. For many years that followed the end of the Cold War and the collapse of the Soviet Union, the US defence establishment was primarily concerned with adversaries whose military capabilities were far smaller than what the United States could bring to bear. Interventions in Somalia, Haiti and the former Yugoslavia were difficult to undertake, but what facilitated them was that the United States and its allies did not have to confront a great power adversary. Similarly, as much as military operations in Iraq and Afghanistan faced numerous problems, the US military was able to use preponderant capabilities to go about missions in a generally permissive environment. That relative sense of ease faded as strategic attention shifted back to great power competition in the 2010s.

A complete intellectual history of MDO is beyond the scope of this report. Suffice it to say that MDO traces its lineage to the last decade of the Cold War. Prior to the 1986 Goldwaters-Nichols Defence Reorganization Act, the armed services of the US military essentially conducted their wartime activities independently of one another. Already a hindrance in the Vietnam War, this division of labour was ill-suited to fighting the numerically superior Warsaw Pact in Central Europe below the nuclear threshold. After all, air power and long-range artillery systems alike would have been indispensable for destroying the reserve units and the rear guard of Warsaw Pact forces in any major armed conflict along the internal German border. Accordingly, the US Army adopted AirLand Battle in 1982 (and NATO in 1984) as its main fighting doctrine for the European theatre, collaborating with the US Air Force to develop the appropriate techniques and procedures, especially concerning close air support and airlift. Despite this improved inter-service dialogue in the 1980s, cultural differences between the two branches prevented closer cooperation. The US Air Force increasingly took the view that air power alone could be strategically decisive. **For its part, the US Army acquired more long-range artillery capabilities that would push out the fire support line where the US Air Force could operate without having to coordinate with ground forces.**[4]

AirLand Battle was—thankfully—never tested in Europe given how the Cold War ended and the Soviet Union collapsed within a decade of its adoption.[5] With the geopolitical environment dramatically different in the 1990s, US military leaders came to believe that digital and information technologies had advanced so much that a new "revolution in military affairs" (RMA) was now afoot. Individual platforms could thus be linked to one another through networks ("system-of-systems") while improvements in sensor technology, intelligence processing and computing power allowed for a massive increase in real-time battlespace awareness.[6] Network-centric warfare—as opposed to platform-centric warfare—became the new paradigm, with the United States asserting by the early 2000s that it had to maintain "full-spectrum dominance" over its adversaries in any military contest. Though the terms "network-centric warfare", "full-spectrum

4 David E. Johnson, "Shared Problems: The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle," RAND, PE-301-A/AF (13 September 2018), p. 4, **https://www.rand.org/pubs/perspectives/PE301.html**.

5 It was doctrine during Operation Desert Storm (1991).

6 William A. Owen, "The Emerging US System-of-Systems," Strategic Forum No. 63 (1996); and Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," US Naval Institute Proceedings, vol. 124, no. 1. (1998): 28-35.

dominance", and "system-of-systems" implied deep integration across multiple combat arms, the services remained divided from one another. The technology was still immature due to insufficient bandwidth and underpowered communication nodes. The connective tissue across a wide range of different platforms was at best thin.

The last fifteen years have seen significant growth in information and communications technology (ICT) such that the aspirations of MDO are much more technically feasible than previous doctrinal efforts during the RMA. Driven by innovations largely made in the private sector, cyber and physical systems have become more integrated thanks to advances in cloud computing, electronic miniaturization, mobile ad-hoc networks (MANETs), wireless sensor networks, big data analytics, machine learning, and cellular networks. Sensors have become ubiquitous: the global sensor market is growing quickly at about eight percent per annum as more and more sensors become embedded with artificial intelligence (AI).[7] Unsurprisingly, the Internet of Things (IoT) has spilt over into the military domain, particularly for logistics and supply chain management, battlespace awareness and communications.[8]

Unfortunately, these technological developments have also empowered potential adversaries to the United States and its allies and partners. The spread of precision strike weapons, the added attention given to the electromagnetic spectrum and the maturity of cyber and information capabilities allow potential adversaries to limit the freedom of manoeuvre that Western militaries might have once enjoyed in places like Afghanistan. Eventually cast as competitors in US policy documents, China and Russia made large investments to modernise their own armed forces using such technologies. With Russia seizing Crimea and destabilising Ukraine in 2014 and China reclaiming islets in the South China Sea where it would later position missile systems, worries abounded among US allies and partners that territory revisionism on the part of authoritarian great powers was back.

Such is the context for the US Army Training and Doctrine Command (TRADOC) assessing that China and Russia developed capabilities and concepts that aimed at undermining US alliances in peacetime and, if necessary, defeating them in wartime. Specifically, TRADOC noted that China and Russia have acquired capabilities to go about stand-off in both peacetime and during armed conflict, with stand-off defined as "the political, temporal, spatial, and functional separation that enables freedom of action in any, some, or all domains, the [electromagnetic spectrum], and the information environment to achieve strategic and/or operational objectives before an adversary can adequately respond."[9] Plainly put, those countries have acquired sufficient missile capabilities that threaten those allied military assets already located within a particular theatre of operations while possibly interdicting those supporting forces that wish to enter that very theatre. Those missile capabilities pose risks to the United States and its allies and partners at sea, on the ground, in the air, as well as in space. Although the US military was already challenging itself to think about "what's after joint?", adversaries are beginning to have at their disposal more sophisticated kill chains, the penetration and neutralization of which will require a deeper level of coordination between services across domains than ever before.[10]

Besides having the potential to disrupt allied defensive efforts, China and Russia could wield those capabilities in their respective regions to estrange the United States and its allies and partners from one another. Breaking up apart those alliances could be achieved in peacetime if those capabilities provoke concerns about the integrity of those alliances themselves or involve a coordinated psychological campaign meant to sow doubt and division within those target societies and their militaries. In a wartime situation, their capabilities could cause significant difficulties for

7 "Sensor Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)," Mordor Intelligence, undated, **https://www.mordorintelligence.com/industry-reports/global-sensors-market**.
8 Mauro Tortonesi et al, "Leveraging Internet of Things Within the Military Network Environment—Challenges and Solutions," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), IEEE (2016): 111-116.
9 Headquarters, TRADOC, The US Army, vi.
10 Jeffrey M. Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," Air & Space Power Journal (Spring 2016): 61.

allied military units in coordinating and working effectively with one another on the battlefield. Of course, for centuries, if not millennia, warfare often involved both the land and sea domains. Arguably all wars involving the great powers have been multi-domain ever since their militaries began flying aircraft and using radios—two technological developments that would give rise to modern combined arms warfare. What renders MDO distinctive, however, is fully integrating and aligning different vectors of military power may be possible due to advances in ICT.

MDO thus serves as a doctrinal framework for a calibrated force posture that allows for manoeuvre and the orchestrated use of military activities across different domains (land, air, sea, cyber, and space). Multi-domain formations in wartime can go about employing cross-domain fires that can optimize effects on the adversary, leading to its eventual disintegration and allowing for an operational breakthrough. According to this vision of MDO, the United States and its allies can outcompete an adversary in peacetime and, if necessary, fight the war effectively on favourable terms.[11] MDO is much more than command and control: since it calls for military forces to operate jointly and in an integrated manner, it requires a particular mindset where different combat arms transcend their service parochialisms and work seamlessly across domains.

Despite the technological promise that MDO can plausibly fulfil, military analysts and commentators writing in the 2010s anticipated several challenges for the doctrinal concept. One challenge relates to inter-service coordination and cooperation.[12] As one retired senior military officer put it, MDO is not so much about providing technical solutions to command and control as it is about fostering a particular "attitude."[13] In the US military, service cultures have historically impeded joint operations because they jealously guarded their own remit. Yet, as David Johnson warned, joint and interagency consensus—both of which are already very difficult—is essential to MDO concept development.[14] The US Army may have first developed MDO, but it has struggled to acquire the full cooperation of the Navy, the Marine Corps, and the Air Force. Those services have their own bureaucratic incentives to resist being told what to do, how to act, and what attitude to adopt by the Army. Still, the Pentagon has been trying to foster greater information-sharing, particularly in the form of Combined Joint All-Domain Command and Control (CJADC2) for troops operating in multiple domains to receive and to use data collected from any of those domains.[15]

Another challenge concerns allied interoperability. The technical ability of long-standing military allies to conduct coalition operations is an old problem. However, MDO risks widening the gap between the United States and its allies. In a 2019 study, Jack Watling and Daniel Roper warn that "if the US does not engage its allies early, and maintain a dialogue about MDO, US capabilities will diverge from allied systems, making the level of integration necessary to achieve convergence unworkable."[16] They highlight the lack of a shared understanding of what MDO is and what it entails, as well as the absence of common systems, particularly with respect to AI and data fusion.[17] **Compounding matters is that several key allies located on Russia's border have militaries that are too small to be organised at higher echelons.**[18] To tailor MDO to their unique circumstances, they are at least obliged to scale down MDO when, according to two military commanders, "the corps is the central echelon in the planning and execution of MDO and is the lowest echelon capable of converging all domains."[19] Simply put, MDO appears to be an intimidating proposition for those countries much smaller in size.

---

11 Andrew Fieckert, "Defence Primer: Army Multi-Domain Operations (MDO)," Congressional Research Service (In Focus, 11409), 2 January 2024.
12 See A.J. Shattuck, "The Pipe Dream of (Effective) Multi-Domain Battle," Modern War Institute, 28 March 2017, **https://mwi.westpoint.edu/pipe-dream-effective-multi-domain-battle/**.
13 Interview with retired senior military officer, Zoom, 14 February 2024.
14 Johnson, "Shared Problems," 6.
15 Colin Demarest, "Pentagon's CJADC2 Milestone is Signal to China, Officials Say," C4ISRNET, 22 February 2024, **https://www.c4isrnet.com/battlefield-tech/c2-comms/2024/02/22/pentagons-cjadc2-milestone-is-signal-to-china-officials-say/**.
16 Jack Watling and Daniel Roper, "European Allies in Multi-Domain Operations," RUSI Occasional Paper (October 2019): 14-17
17 Ibid.
18 Watling and Roper, "European Allies."
19 Andreas Marlow and Wilson C. Blythe, "Multi-Domain Warfighting in NATO: The 1 German-Netherlands Corps View," Military Review (May-June 2022): 21.

2. MDO in the Context of Russia's Full-Scale Invasion of Ukraine

Of the two countries that the United States now designates as its great power competitors, only Russia has been engaged in high-intensity combat operations given the full-scale invasion of Ukraine it initiated on 24 February 2022. Moreover, the European security environment has sharply deteriorated since TRADOC published its doctrinal statement on MDO in 2018. Though it experienced severe operational setbacks throughout 2022, especially in the Kyiv and Kharkiv regions, Russia seized significant amounts of territory in the southern and eastern parts of Ukraine. Its aims remain explicitly maximalist, with Russian leaders repeatedly calling for the destruction of the Ukrainian state while occasionally making nuclear threats to NATO countries to deter them from providing military assistance to their beleaguered partner.

The Russian Armed Forces (RAF) have suffered massive losses, but they have successfully reconstituted units that have suffered high attrition rates. The RAF has expended significant ammunition and used large numbers of ballistic and cruise missiles, but it continues to put immense pressure on Ukraine thanks to assistance from Iran and North Korea. Russia's economy has come under severe stress and raised questions about its long-term prospects. However, Russia has largely orientated its economy to service its war.

The record of Russia's military performance affords an opportunity to appraise the original threat assessment that shaped much of pre-2022 MDO thinking. Specifically, was Russia able to achieve a "stand-off" vis-à-vis Ukraine, whether to isolate it from its Western partners or to prevent Ukrainian military units from operating effectively in battle? The discussion considers three sets of capabilities in turn—electronic warfare (EW), missile capabilities, as well as cyber and information—and concludes that Russia's own military performance has validated some earlier MDO thinking even if Russia has struggled in achieving its main operational goals.

Russian Electronic Warfare

The first point of validation relates to Russia's EW capabilities. EW refers to "[any] military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy," with the electromagnetic spectrum (EMS) encompassing radio waves, microwaves, infrared, visible light, ultraviolet light and ionizing radiation.[20] Russia has developed EW capabilities to jam communications, enhance situational awareness, use radiated electromagnetic energy to identify threats and protect its own forces from the adversarial use of EW. Like various NATO members, it has coupled EW capabilities with cyber capabilities, improving data links between systems as well as engaging in greater deception and disruption of enemy systems.[21]

Regarding Russia's full-scale invasion of Ukraine, pre-February 2024 expectations were that Russia was highly adept in EW. Russia did succeed at first in using its electronic attack systems and aerial decoys to force Ukrainian air defence systems offline. Ukrainian air defence radar was jammed, as were Ukrainian aircraft in their use of air-to-ground and air-to-air communications.[22] Internet connectivity was, and remains, a persistent problem for the Ukrainian Armed Forces. However, many Russian military communications within Ukraine were unencrypted while Ukrainian air defences recovered from the initial onslaught to

20 US Department of Defence, Joint Publication 3-85 – Joint Electromagnetic Spectrum Operations (Washington, DC: US Department of Defence, 2020): GL-9. For a helpful discussion, see Thomas Withington, "Manoeuvre Warfare and the Electronic Spectrum," The RUSI Journal, vol. 168, no. 6 (2023): 32-41.

21 Roger N. McDermott, Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum (Tallinn, Estonia: International Centre for Defence and Security, 2017); and Duncan McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States," The RUSI Journal, vol. 165, no. 7 (2020): 34-44.

22 Jack Watling, The Arms of the Future: Technology and Close Combat in the Twenty-First Century (London, UK: Bloomsbury, 2024): 38; and Mykhaylo Zabrodskyi, Jack Watling, Oleksandr V. Danylyuk, and Nick Reynolds, Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022 (London: Royal United Services Institute, 2022): 30.

force Russian fixed- and rotary-winged aircraft to fly dangerously at low altitudes.[23] Eventually, Russian EW also recovered to tip the balance back in favour of Russia, with Ukrainian units becoming exposed to drone-guided artillery strikes and Western-supplied precision munitions missing their targets.[24] This was evident even during 2022, as Russia demonstrated its ability to adapt in EW. Ukraine captured a Krasukha-4 command module system in March 2022, leading observers to declare that its loss "could be significant for Russian forces from an operational perspective."[25] Yet, this loss turned out to be far less consequential than what was initially believed.[26] As one report concludes, "it is essential to actively contest the EMS," not least because "whichever side can secure better access to the EMS is likely to retain significant tactical advantages that accumulate over time."[27]

Russian Missile Capabilities

With some caveats, the second point of validation concerns Russia's use of its own missile capabilities. Before 2022, much military discussion centred on the so-called anti-area and anti-access (A2AD) problem that Russia's missile and other systems had posed in the Baltic and Black Seas. Although A2AD itself is a Western construct that is absent in Russian military concepts and doctrines, the A2AD problem was defined as follows: Russia had deployed significant coastal, air defence and anti-submarine systems in Kaliningrad and Crimea that would not only protect Russian-held territory but also severely inhibit the movements of an opposing military coalition. Stand-off missile systems—3M-14 Kalibr land-attack cruise missiles, P-800 Oniks surface-to-surface anti-ship cruise missiles, Iskander short-range ballistic missiles and the S-400 Triumf surface-to-air missiles—have afforded greater defence-in-depth for Russia by increasing its ability to do interdiction and potentially to deter reinforcements located from outside the theatre-of-operations.[28] Those stand-off capabilities could thus 'decouple' frontline NATO members from their more westerly allies.

Already before 2021, analysts expressed scepticism regarding the notion that Russian missile capabilities would accomplish those goals as effectively as often argued, noting the exaggerated ranges of certain Russian air defence systems and other technological limitations.[29] The full-scale attack that began in February 2022 did see Russia expend large numbers of missiles to attack critical Ukrainian infrastructure and urban centres, forcing Kyiv to prioritise acquiring western air defence systems and interceptor missiles. While repeated large-scale missile strikes against Ukraine have arguably not yielded strategic gains, this could change since repeated missile attacks in the spring of 2024 have depleted Ukraine's air defences.

Still, Ukrainian support for the war and belief in final victory remain very strong.[30] Importantly, as of May 2024, the Russian Black Sea Fleet—responsible for lobbing many missiles at Ukrainian targets—lost a fifth of its surface vessels to Ukrainian missile and drone strikes, flipping the so-called Russian A2AD challenge on its head.[31] Ukraine successfully dislodged Russia from Snake Island thanks to ground-based artillery. Russia also experienced severe difficulties interdicting military supplies flowing into Ukraine from its NATO partners.[32] Of course, none of this is to say that Russian missiles have had no effect whatsoever. They have imposed terrible costs, inflicting heavy losses of human life and destroying much

---

23 Duncan McCrory, "Electronic Warfare in Ukraine: Preliminary Lessons for NATO Air Power Capability," The Journal of the JAPCC (2023): 69-74.

24 Roman Olearchyk, "Military Briefing: Russia Has the Upper Hand in Electronic Warfare with Ukraine," Financial Times, 7 February 2024, **https://www.ft.com/content/a477d3f1-8c7e-4520-83b0-572ad674c28e**. Russia has arguably been engaging in EW against NATO around the Baltic region throughout early 2024. See

25 Joseph Trevithick, "Ukraine Just Captured Part of One of Russia's Most Capable Electronic Warfare Systems," The War Zone, 22 March 2022, **https://www.twz.com/44879/ukraine-just-captured-part-of-one-of-russias-most-capable-electronic-warfare-systems**.

26 My thanks to Davis Ellison for this point.

27 Zabrodskyij et al, Preliminary Lessons, 60-61.

28 Keir Giles and Mathieu Bouleque, "Russia's A2/AD Capabilities: Real and Imagined," Parameters, vol. 49, no. 1 (2019): 24.

29 See Robert Dalsjö, Christofer Berglund, and Michael Jonsson, Bursting the Bubble: Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications, FOI-R--4651-SE (Stockholm: Swedish Defense Research Agency [FOI], 2019); and Giles and Boulegue, "Russia's A2/AD Capabilities."

30 Alexander Motyl, "Why Ukrainians Are Still So Optimistic," The Hill, 26 February 2024, **https://thehill.com/international/4489674-why-ukrainians-are-still-so-optimistic/**.

31 Yuri Zoria, "Ukraine Intel Destroys Another Russian Navy Ship "Sergei Kotov" (Updated)," Euromaidan Press, 5 March 2024, **https://euromaidanpress.com/2024/03/05/ukraine-intel-says-it-destroyed-another-russian-navy-ship-sergei-kotov/**.

32 Stetson Payne and Tyler Rogoway, "Weapons Shipments are in Russia's Crosshairs After Missiles Hit Ukrainian Border Base," The War Zone, 13 March 2022, **https://www.twz.com/44730/its-clear-weapons-shipments-are-now-in-russias-crosshairs-after-missiles-hit-ukrainian-border-base**. NATO military assistance expanded significantly over the course of 2022. See Alexander Lanoszka and Jordan Becker, "The Art of Partial Commitment: The Politics of Military Assistance to Ukraine," Post-Soviet Affairs, vol. 39, no. 3 (2023): 173-194.

infrastructure. For this reason, NATO members themselves expanded their own investments in such systems since 2022.[33]

Russian Cyber and Information Activities

The record of Russian cyber and information activities against Ukraine since 2022 has been much more mixed. Before the full-scale invasion, many experts assessed that Russia developed a significant cyber capability that could deliver strategic effects. Keir Giles, for example, warned that "a destructive cyber onslaught could target military command and control systems or civilian critical infrastructure and pressure Kyiv into concessions and its friends abroad into meeting Russia's demands."[34] Others noted that Russia had developed significant "communication power" to use its extensive presence on traditional and social media to broadcast its preferred narratives and to shape political discourse abroad.[35] Before and during its full-scale invasion, Russia undertook malicious cyber activities against Ukraine and various NATO allies while trying to promote its own narratives about its war-making to global audiences.

Its cyber and information nevertheless fell short of expectations. Nadiya Kostyuk and Erik Gartzke argue that Russian cyber-attacks did not achieve strategic gains, not least since defaced websites were quickly restored and Ukrainian data remained largely secure.[36] Internet connectivity within Ukraine persisted, especially after Starlink came online.[37]

That said, as mentioned above, Ukrainian military units have suffered connectivity issues. In the information space, most governments in Europe moved to shut down Russian propaganda outlets while Ukrainian President Volodymyr Zelenskyy channelled his energies to shaping global perceptions of the conflict and encouraging the provision of military assistance.[38] Although Russia received some support in parts of the developing world, its overall communication power appears much diminished. As the war became more positional and other violent conflicts diverted global media attention, however, Russia made headway in the information space once more.[39] The US Congress's reluctance to provide additional military assistance to Ukraine in early 2024 cruelly exposed the limits of Ukraine's narrative power.[40] The Biden administration has sometimes justified its hesitation to send specific types of weapons or their configurations to Ukraine based on perceived escalation risks, thereby suggesting that Russia may indeed have achieved some "stand-off".[41]

Summary

Put together, Russia's performance in its own full-scale invasion of Ukraine occasions some reconsideration of MDO's founding threat assessment. Recall that this threat assessment had Russia capable of achieving decisive strategic effects at the expense of US allies and partners thanks to its missile arsenal in addition to its EW, cyber and information capabilities. The record of Russia's war-making has mostly validated the fundamental precepts of that threat assessment despite how Ukraine's fierce resistance has shown that some of those apparent Russian strengths were overstated. Russian electronic warfare has proven highly problematic for the Ukrainian Armed Forces. Russian missile and drone strikes against Ukraine have caused massive infrastructural damage and the loss of many lives. Considering

---

33 See "10 NATO Allies take further step to boost European air and missile defence capabilities," NATO, 11 October 2023, **https://www.nato.int/cps/en/natohq/news_219119.htm**.

34 Keir Giles, "Putin Does Not Need to Invade Ukraine to Get His Way," Chatham House, 6 December 2021, **https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way**.

35 James Rodgers and Alexander Lanoszka, "Russia's Rising Military and Communication Power: From Chechnya to Crimea," Media, War & Conflict, vol. 16, no. 2 (2023): 135-152.

36 Nadiya Kostyuk and Erik Gartzke, "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine," Texas National Security Review, vol. 5, no. 3 (2022) 113-126. On Russian cyber activities against Ukraine, see Aaron F. Brantly and Nataliya D. Brantly, "The Bitskrieg That Was and Wasn't: The Military and Intelligence Implications of Cyber Operations during Russia's War on Ukraine," Intelligence and National Security (2024): doi:10.1080/02684527.2024.2321693.

37 Rachel Lerman and Cat Zakrzewski, "Elon Muk's Starlink Keeps Ukrainians Online When Traditional Internet Fails," The Washington Post, 19 March 2022, **https://www.washingtonpost.com/technology/2022/03/19/elon-musk-ukraine-starlink/**.

38 See Olga Onuch and Henry Hale, The Zelensky Effect (New York: Oxford University, 2022); and Anastasiia Kapranova, The Role of Strategic Communications in Shaping 'Western' Military Aid to Ukraine Amidst Russia's War of Aggression (M.A. thesis: College of Europe in Natolin, 2023).

39 "Russia's Pockets of Support are Growing in the Developing World," Economist Intelligence Unit, 7 March 2023, **https://www.eiu.com/n/russias-pockets-of-support-are-growing-in-the-developing-world/**.

40 See Alex Finley, "Russia Is Buying Politicians in Europe. Is It Happening Here Too?" The New Republic, 12 April 2024, **https://newrepublic.com/article/180630/russia-corruption-network-europe-buying-politicians-america**.

41 For an approving assessment of the Biden administration's approach, see Janice Gross Stein, "Escalation Management in Ukraine: "Learning by Doing" in Response to the "Threat that Leaves Something to Chance,"" Texas National Security Review, vol. 6, no. 3 (2023): 29-50.

that much of NATO's eastern flank does not have the geographical depth of Ukraine, the margin of error is much tighter for them, particularly in the opening stages of an invasion by a reconstituted and highly determined Russia.

One additional observation must be made. What ultimately denied Ukraine the ability to achieve success in its 2023 counteroffensive was the extensive system of fortifications that Russian army engineers were able to build on occupied territory since the autumn of 2022. Defensive works like those fortifications received little attention in Western military thinking prior to the full-scale invasion, even though walls and other physical barriers were already becoming commonplace around the world.[42] Many formulations of MDO gave little, if any, consideration to the issue of fortifications. In the context of the Eastern flank, however, such an oversight must be corrected.

42 David J. Betz, The Guarded Age: Fortification in the Twenty-First Century (Cambridge, UK: Polity, 2024)

3. MDO along the Eastern Flank

Much of the US Army's focus on MDO has implicitly centred on potential military scenarios in the Baltic littoral region.[43] This is largely due to Russia's significant military presence in the Kaliningrad exclave, which poses notable standoff capabilities. Estonia, Latvia, and Lithuania find themselves effectively isolated, huddled between the Baltic Sea and Russia's European territory. The only land connection these Baltic countries have to the rest of NATO is the short border between Lithuania and Poland, which separates the Kaliningrad exclave from Belarus. This critical border area is often referred to as the "Suwałki Gap" or the "Suwałki Corridor", raising concerns that Russia would attempt to seize it in a bid to isolate the Baltic countries and hinder NATO reinforcements. Given Russia's numerical military advantage and the geographical challenges of the Baltic region, there is a risk of NATO allies being divided during peacetime.[44] If an armed conflict were to break out, Russia could leverage these military advantages to make major strategic gains and disrupt allied defensive efforts.

The implicit scenarios guiding US Army strategy align with the significant geostrategic attention that NATO now pays to its so-called Eastern flank. NATO's eastern flank comprises countries along the Alliance's eastern frontier, from Finland in the north to Bulgaria and Romania in the south. Most discussions of the Eastern flank centre specifically on Poland and the three Baltic countries, due to their shared land borders with Russia and their NATO membership before Russia's 2014 incursion into Ukraine. Their heightened threat perceptions have led them to recapitalise their armed forces following Russia's seizure of Crimea. Accordingly, they have been procuring new military equipment while expanding their personnel numbers.[45]

The Eastern flank has been the focal point for many deterrence and defence measures that, taken together, are effectively multi-domain. The enhanced Forward Presence (eFP) comprises multinational battlegroups that unite ground units from across the Alliance to the eastern flank. First established in 2004 but strengthened since 2014, the Baltic Air Policing is an air defence mission aimed at early warning, surveillance and airspace control over Estonia, Latvia, and Lithuania. Despite their small size, the Baltic countries have benefited from allied ships participating in Standing NATO Maritime Group 1 that patrol the Baltic Sea and engage in joint military exercises that test operational readiness. Estonia and Latvia are leaders in cyber and information warfare, respectively, hosting two centres of excellence in their capital cities. Moreover, the Lithuanian government has circulated manuals to its population on what to do in the event of a major national emergency.[46] The Baltic countries are promoting volunteer forces to enhance social resilience to varying degrees.[47]

MDO is highly relevant to NATO's eastern flank. However, conversations with officials and experts indicate a lack of explicit consideration of MDO.[48]As indicated below, official defence documents generally do not directly mention MDO. This gap is surprising since MDO partly serves to improve the defence of the Baltic region and hinder Russia's ability to achieve wartime objectives if it escalates militarily against NATO.

Some analysts may argue that the absence of explicit discussion onMDO may not necessarily be detrimental. In a comprehensive 2023 study by Davis Ellison and Tim Sweijs on how various NATO members conceive and implement MDO, they raise six separate concerns. Firstly, they highlight the diverse interpretations of MDO among different countries and their respective

43 Davis Ellison and Tim Sweijs, Breaking Patterns: Multi-Domain Operations and Contemporary Warfare (The Hague, NL: The Hague Centre for Strategic Studies, 2023): 27.
44 For an earlier but flawed assessment to this effect, see David A. Shlapak and Michael W. Johnson, Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics (Santa Monica, CA: RAND Corporation, 2016).
45 Alexander Lanoszka, Will the Eastern Flank be Battle Ready? Deterrence by 2030 (Bratislava, SK: GLOBSEC, 2023).
46 Lionel Beehner and Liam Collins. "Can Volunteer Forces Deter Great Power War? Evidence from the Baltics," Journal of Strategic Security, vol. 12, no. 4 (2019): 61.
47 Beehner and Collins, "Can Volunteer Forces ...?"
48 They focus specifically on MDO development and implementation in Denmark, France, Germany, Israel, NATO, Taiwan, the United Kingdom, and the United States. They chose those NATO members due to their relevance to the Dutch military context. They chose Israel and Taiwan because of how they are small states facing very precarious security environments.

armed forces branches. Secondly, they argue that MDO often clashes with the structures of civil-military relations and national defence establishments. Thirdly, they warn that MDO relies on an overly optimistic view of what existing technology can provide. Fourthly, they critique the vague naturethreat assessments driving MDO development and implementation. Fifthly, they note that MDO suffers from an underdeveloped theory of victory. Finally, they worry that developers and operators may not fully comprehend the inherent trade-offs involved in designing war-fighting concepts or military capabilities.[49]

Rather than develop these critiques, I group the issues raised by Ellison and Sweis into three broad considerations, framed as questions, to organise the discussion below. First, to what extent and how do eastern flank militaries articulate and incorporate MDO concepts? Second, how are eastern flank militaries thinking of connectivity, broadly defined, whether between parts of government, military units and the platforms themselves? Third, how should eastern flank countries organise and test their MDO within the context of an operational campaign? This section is organised around these three considerations.

1. *To what extent and how do eastern flank militaries articulate and incorporate MDO concepts?*

Analysts have noted that those NATO defence establishments—typically those in North America and Western Europe—that do articulate MDO concepts often disagree on how they define and interpret key ideas.[50] These disagreements can even exist within militaries as different combat arms and services develop MDO ideas in accordance with their own bureaucratic interests or cultural practices. Larger countries may contribute most to the proliferation of terms and concepts, as their defence establishments involve a greater number of stakeholders. The core issue is that unclear language has led to divergent assessments for treating particular problems and has caused miscommunication between interlocutors.

Cacophony and concept proliferation do not appear to be issues with the eastern flank, however. Instead, silence is more typical of the region. Despite the breadth of these measures and the inherent multi-domain challenge that exists in the Baltic littoral region, MDO thinking remains underdeveloped across local national defence establishments. Estonia's 2023 National Security Concept does not refer to Multi-Domain Operations, even though it emphasises the importance of citizens' preparedness in the face of Russian threats. It highlights how "Estonia is developing manoeuvre units and territorial defence units capable of blocking and countering the adversary," adding that 'situational awareness, advanced early warning, capable intelligence, counterintelligence and a shared threat perception amongst Allies are key to ensuring efficient national defence planning and pre-empt military threats."[51] The Latvian State Defence Concept (2023-2027) makes no explicit mention of Multi-Domain Operations. It does note that Russia uses "energy, migration, and other increasingly innovative means of hybrid warfare" against Western countries and that, in wartime, it could use "an overwhelming superiority characterised by a massive infantry offensive, new and inexpensive technologies, and artillery firepower."[52] Lithuania has released no public document that directly tackles MDO *(daugiadėmenėms operacijoms)*.

MDO (operacje wielodomenowe) thinking is more advanced in Poland. One reason may be the significant presence of the US Army, particularly through its participation in the local eFP (or Multinational Brigade) Battlegroup and elsewhere in Polish territory. Another reason is that the Polish Armed Forces is significantly larger than its Baltic countries, with many big-ticket procurement decisions that include numerous M142 High Mobility Artillery Rocket Systems (HIMARS), 32 F-35A Block 4 fighter jets, a multitude of M1A2 SEP v3 and K2

49 Ellison and Sweijs, Breaking Patterns, ii-v.
50 Ellison and Sweijs, Breaking Patterns, 21-23.
51 Republic of Estonia, National Security Concept of Estonia, 2023, 14.
52 Republic of Latvia, The State Defence Concept (2023-2027), 5

tanks, and three Miecznik-class multi-role frigates. It also has been pursuing an air defence programme (called "Wisła") with different component parts that will integrate with one another to cover various ranges and types of threats. Indeed, air defence is one area where MDO thinking is arguably the most explicit in the Polish context.[53] The extensive use of drones in the Russo-Ukrainian War also seems to be encouraging MDO thinking in the Polish Armed Forces.[54] Effective integration of these platforms is essential. For instance, the F-35 can act as a sensor to relay data for HIMARS operators, allowing them to accurately target enemy positions.

The 2020 Polish National Security Strategy pays particular attention to recent technological developments. It notes that the "[d]evelopment of solutions based on fixed line and mobile broadband (5G and subsequent generations), the Internet of Things, cloud computing, quantum technologies, automation of services, machine learning, nanotechnology and artificial intelligence create new 8 development opportunities for Poland, while generating previously unknown threats."[55] The Strategy proceeds to emphasise the need to "strengthen the operational capabilities of the Polish Armed Forces by increasing personnel and equipment to the foreseen levels, as well as adapt training programmes to respond in particular to the challenges presented by the modern multi-domain operational environment, capabilities to conduct asymmetric operations, building Anti-Access/Area Denial systems (battlefield isolation) and manoeuvrability of operations, as well as the ability to stay away from permanent dislocation for a lengthy period of time."[56]

As for other NATO allies on the eastern flank, there is significant variation. Slovakian defence documents do not mention MDO. Neither do Romanian ones, although there is some scholarship produced in Romania that reflects on MDO.[57] Hungary does not formally consider MDO, even though its national security strategy recognises the increased importance of precision-strike, information communications technology and interconnectedness. Endorsed legislatively in 2021, Bulgaria's Programme for the Development of the Defence Capabilities of the Bulgarian Armed Forces fails to mention MDO explicitly.[58] Finland is currently revising its national security strategy, no doubt prompted by its successful accession to NATO following Russia's full-scale invasion of Ukraine.[59] Since it is new to NATO, MDO has to date been absent in formal documents.

Whatever the content of various policy and doctrinal documents, joint military exercises conducted over the last decade in and around the Baltic Sea region have been essentially multi-domain in form. For example, STEADFAST DEFENDER 2024, held in the northern areas of Norway, Sweden and Finland, comprised tactical military exercises that spanned the land, air, sea, cyber and space domains.[60] However, two critical observations about these military exercises must be made. Firstly, **some NATO military exercises seem to lack realism, reflecting perhaps a tendency to avoid embarrassing blue forces**. One anecdote relates that, during Exercise HEDGEHOG in Estonia, "being so busy watching the jets overhead [at 500 ft], enemy forces completely miss the huge vehicles making advances behind them."[61] Although celebrated as an example of good multi-domain integration, the anecdote invites the question as to why a military force would invade NATO territory but be overawed by NATO aircraft making themselves extremely vulnerable to SHORAD. For such military exercises

53 Jakub Palowski, "IBCS as the Foundation for Multi-Domain Air Defense," Defence24, 24 September 2021, **https://defence24.com/armed-forces/bcs-as-the-foundation-for-multi-domain-air-defense**.

54 Maciej Szopa, "Defence24 Day: Operacje wielodomenowe w Siłach Zbrojnych RP," Defence24, 27 May 2022, **https://defence24.pl/polityka-obronna/defence24-day-operacje-wielodomenowe-w-silach-zbrojnych-rp**.

55 Biuro Bezpieczeństwa Narodowego (BBN, National Security Bureau), National Security Strategy of the Republic of Poland (2020), 7-8, **https://en.bbn.gov.pl/en/about-bbn/publications/publications/769,National-Security-Strategy-of-the-Republic-of-Poland.html**. A new security strategy appears to be in the offing as a result of Russia's full-scale invasion of Ukraine and the change of government in Poland. "MON zapowiedziało stworzenie nowej doktryny obronnej Polski. "Obecne dokumenty są nieaktualne", Polskie Radio, 29 February 2024, **https://polskieradio24.pl/artykul/3342591,mon-zapowiedzialo-stworzenie-nowej-doktryny-obronnej-polski-obecne-dokumenty-sa-nieaktualne**.

56 BBN, National Security Strategy, 18.

57 See, e.g., Alexandru-Lucian Cucinschi, "The Impact of Multi-Domain Operation on the Military Strategy," Romanian Military Thinking 1 (2021): 140-151.

58 Programme for the Development of the Defence Capabilities of the Bulgarian Armed Forces, endorsed by the 44th National Assembly, 11 February 2021.

59 "Finnish Government to Draw Up National Security Srategy," Finnish Government, 8 March 2024, **https://valtioneuvosto.fi/en/-//1410869/finnish-government-to-draw-up-national-security-strategy**.

60 "The JWC's Multi-Domain Scenario Support for NATO Exercise STEADFAST DEFENDER 2024," NATO, 6 February 2024, **https://www.jwc.nato.int/articles/jwcs-all-domain-scenario-support-nato-exercise-steadfast-defender-2024**.

61 Sophie Barnes, "Multi-Domain Integration: Learning From One Another to Become Stronger Together," NATO, 3 August 2023, Baltic Amber (NATO), **https://mncne.nato.int/baltic-amber-magazine/multidomain-integration-learning-from-one-another-to-become-stronger-together**.

to be credible, red teams should not follow a particular script that gives blue teams artificial advantages.[62]

The second problem affecting the quality of MDO military exercises in the Baltic region is their technical complexity and expense. The airspaces available in Europe for training are limited and highly constrained, especially for newer-generation aircraft. Testing highly networked, MDO-enabled capabilities is a major challenge. **Europe's small and densely populated subcontinent makes it difficult to simulate EW in military exercises meaningfully without risking any degradation or disruption to civilian operations.** Although quantum computing may eventually become available for very sophisticated MDO simulations, the bandwidth necessary would be inordinate. Virtual training can supplement practical exercises, but it is no substitute for hands-on, practical training.[63]

2. *How are eastern flank militaries thinking of connectivity, broadly defined, whether between parts of government, military units, and the platforms themselves?*

If they are not thinking about MDO per se, defence establishments along the eastern flank are starting to think about connectivity, albeit unevenly. Cyber is integral in this regard. In the last decade, experts have called attention to the Internet of Military Things (IoMT). Connecting platforms and pieces of equipment can enhance situational awareness through intelligence gathered through sensors. Logistical operations can become more efficient, and medical care can be more responsive and timelier.[64]

Consider the following scan of security and defence documents governments across the eastern flank have produced. Poland's Cybersecurity Strategy is most aligned with MDO, asserting that "the ability to do the full spectrum of military activities in cyberspace must therefore involve, among other things, threat recognition, security and defence of networks and ICT systems as well as fighting the sources of cyberthreats." It proceeds to emphasise how Poland must boost its military posture in the cyber domain in the pursuit of these tasks.[65] Released in 2019, Lithuania's National Cyber Security Strategy declares that "national cyber defence capabilities will be developed by ensuring interaction between the Lithuanian Armed Forces and the country's civil capabilities, also capabilities of the Lithuanian Armed Forces to ensure reliable deterrence of aggressors in cyber space." It adds that, if necessary, "the Lithuanian Armed Forces would defend the Republic of Lithuania by using military cyber security measures acting autonomously and in cooperation with allies."[66] Bulgaria recognises cyber as its military domain and the need for interoperability, warning that emerging disruptive technologies "pose risk of creating a significant technological gap between the Armed forces of different Allies, which might have a negative impact on interoperability and the ability to conduct joint operations."[67] Bulgaria thus aspires to develop AI-based systems for the extraction, processing, analysis and dissemination of information across multiple domains.[68] Hungary's 2021 National Military Strategy declares that "[a]dvanced, network-based, autonomous command and control capabilities will be developed that can be effectively operated even in technologically underdeveloped, non-supportive environments." It adds that "[h]igh-bandwidth jamming-proof, unclassified and secured data connections; the protection of forces' information communications networks against cyber and electronic warfare; and the readiness for intragovernmental cooperation capabilities must be provided."[69]

No such statements appear in the documents

62 See also Micah Zenko, "Millenium Challenge: The Real Story of a Corrupted Military Exercise and its Legacy," War on the Rocks, 5 November 2015, **https://warontherocks.com/2015/11/millennium-challenge-the-real-story-of-a-corrupted-military-exercise-and-its-legacy/**.
63 Interview with former senior US military official, 14 February 2024.
64 Konrad Wrona, "Securing the Internet of Things: A Military Perspective," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE (2015): 502-507.
65 Ministry of Digitalisation of the Republic of Poland, Cyber Security Strategy of the Republic of Poland for the Years 2019-2024 (2019): 24. Author's translation.
66 Ministry of Defence of the Republic of Lithuania, Lithuania National Cyber Security Strategy (2019): 9.
67 Programme for the Development of the Defence Capabilities of the Bulgarian Armed Forces, endorsed by the 44th National Assembly, 11 February 2021, 9.
68 Ibid, 15.
69 Government of Hungary, National Military Strategy of Hungary, 13 October 2021.

of other eastern flank countries. **Latvia's Cybersecurity Strategy specifies five activity directions, mostly civilian-focused, including cybersecurity governance, enhancing the resilience of public and private systems, increasing public awareness, protecting human rights, upholding the rule of law in cyberspace and addressing cyber crime.**[70] Romania's 2013 Cyber Security Strategy explicitly focuses on coordinating cyber security activities across government as well as with EU and NATO initiatives, emphasising countering cyber attacks and protecting critical infrastructure. Very little is explicitly military in the document.[71] Still, these null results have caveats: in practice, regardless of what specific documents might say, defence establishments may still be going about addressing issues of interconnectivity and securing ICT systems.

The content of these documents aside, one advantage that eastern flank countries might have over their Western European allies is that they appreciate how intertwined civilian efforts are with military operations. A feature of the Russo-Ukrainian War has been the deep involvement of many Ukrainian civilians in resisting Russian aggression, whether by information sharing, assisting territorial defence units, provisioning supplies or engaging in hactivism.[72] The war has demonstrated that military operations cannot rely solely on military infrastructure and that some degree of collaboration with civilian society is essential. Already in Finland, the concept of "total defence" calls for civilian preparedness in the event of a national emergency.[73] Along similar lines, Lithuania announced its intent in early 2022 "to build citizens' resilience to prevent a potential aggressor, for example, from carrying out information attacks [or] cyber attacks."[74] Estonia approved a framework document in February 2024 aimed at enhancing civil defence, involving such measures as improving warning times and crisis medicine and management skills.[75] One stated purpose of Poland's recently formed Territorial Defence Force has been to improve social resiliency. Although these measures may not necessarily aim at connectivity in the EMS domain, they still serve to strengthen the military-civilian nexus where practicable.

In short, countries across the eastern flank are recognising the importance of connectivity across military platforms and the military-civilian divide, even if they do not explicitly use MDO termnology. That said, the solution to modern military problems is not simply "more connectivity". A challenge with any armed force and ICT will ultimately be organisational. As Jon Lindsay observes, "military organisations have become more dependent on information technologies and experienced more coordination problems."[76] Indeed, Lindsay cautions that connectivity challenges will remain despite the promise of technology. Data fusion has become more automated, but conflicts themselves are becoming more ambiguous, more fluid and prone to technological change as well. Problems of judgment will become more significant since human operators still need to make decisions regarding the interpretation, sharing and the use of data generated on the battlefield. National defence establishments need to be mindful of the human element involved.[77]

3. *How should eastern flank countries organise and test their MDO in terms of an operational campaign?*

What should facilitate MDO development and implementation in the eastern flank context is the widespread agreement that Russia represents the most profound military threat. This consensus

70 Ministry of Defence of the Republic of Latvia, Cybersecurity Strategy of Latvia, 2023-2026 (2022): 17-29.
71 National Cyber Security System, Cyber Security Strategy of Romania, Romania (2013).
72 Marta Kepe and Alyssa Demus, "Resisting Russia Insights into Ukraine's Civilian-Based Actions During the First Four Months of the War in 2022," RAND Research Report, 15 August 2022, **https://www.rand.org/pubs/research_reports/RRA2034-1.html**.
73 Richard Milne, "War with Russia? Finland has a Plan for That," Financial Times, 28 March 2022, **https://www.ft.com/content/c5e376f9-7351-40d3-b058-1873b2ef1924**.
74 BNS, "Lithuanian government approves strategy to prep society for resistance," LRT, 26 January 2022, **https://www.lrt.lt/en/news-in-english/19/1598501/lithuanian-government-approves-strategy-to-prep-society-for-resistance**.
75 "Government Approves Civil Defence Objectives and Action Plan," Stenbock House, 22 February 2024, **https://www.valitsus.ee/en/news/government-approves-civil-defence-objectives-and-action-plan**.
76 Jon R. Lindsay, "The Economic Complements of AI and the Political Context of War," in Responsible Use of AI in Military Systems, ed. Jan Maarten Schraagen (Boca Raton, FL: Chapman and Hill, 2023): 303.
77 Lindsay, "The Economic Complements."

has remained intact despite some multi-domain capabilities being overstated before 2022. The United States, the United Kingdom and France face a wider set of military challenges because of their global reach, forcing them to consider hard choices about which threats to prioritise and the trade-offs that might ensue as they go about the development of their war-fighting concepts and defence procurement. Many other Western European countries are geographically distant from Russia but face other geopolitical considerations. The Baltic region is undoubtedly a complex environment due to the significance of the Baltic Sea, the mass that Russia can bring to bear and the relative geographical isolation of the Baltic countries. However, what simplifies the Baltic region—and the rest of the eastern flank—is that there is just one adversary that can only launch a military attack in several plausible ways. Certain concerns that some analysts have raised concerning MDO and riskiness should be moot.

One observation from the Russo-Ukrainian War relates to the importance of fortification. Russian military units gathered in Crimea were able to stream into the Kherson and Zaporizhzhia Oblasts in February and March 2022 partly because they faced no physical barriers by way of minefields and trenches. In contrast, the much-hyped Ukrainian counteroffensive in the summer of 2023 failed to deliver due to the system of fortifications that Russian forces constructed in the preceding months. For their part, advancing Russian armoured columns have experienced their own difficulties overcoming Ukrainian defensive lines.

Poland and the Baltic countries have apparently learnedthat fortification is effective and worthy of investment. In the spring of 2024, Poland announced its intent to develop the "Eastern Shield" (tarcza wschód) along the border with both Belarus and Russia. The 10-billion PLN plan envisions improved early warning systems, anti-drone systems and various counter-mobility measures.[78] The Polish government aims to link the "Eastern Shield" with the Baltic Defence Line, which the Baltic countries had declared their intent to build earlier in 2024. Being mindful of the peaceful uses of the land, the three governments agreed not to use explosives (e.g., mines), cutting wires and dragon's teeth until a military crisis breaks out. Such equipment would instead be stored nearby.[79] Estonia plans to build 600 bunkers that can each contain a platoon of ten soldiers while being able to absorb a direct hit from 152mm calibre shells. The plan is ambitious. If Latvia and Lithuania build fortifications at the same density as Estonia along their land border with Russia, they would have to construct 1,116 and 2,758 bunkers, respectively.[80] Such numbers are likely unnecessary considering the relatively few crossing roads and rail links that Russia could exploit and, for that matter, would need to go about an invasion and sustaining it logistically.[81]

At first glance, the Baltic Defence Line and Poland's "Eastern Shield" appear to be at odds with MDO. Fortification is by nature static, whereas MDO emphasises manoeuvre at echelon. However, these fortification projects can and should be aligned with MDO. Consider their potential effects on the attacker. Firstly, a large-scale incursion like Russia's invasion of Ukraine in 2022 is unlikely to achieve operational surprise.[82] Russia's invasion was preceded by the movement of significant equipment to positions near the Ukrainian border, visible through satellite imagery and social media footage, indicating operational significance. Pre-positioning equipment for an invasion takes time, thereby providing much early warning that in turn can allow the Baltic countries to make the necessary preparations along the Baltic Defence line.[83] The Baltic Defence Line, along with Poland's 'Eastern Shield', can further hinder Russia's ability to achieve strategic surprise because Russia may have to resort to artillery barrages to prepare the battlefield, which in turn

78 Piotr Kozłowski, "Największa operacja umacniania wschodniej flanki NATO. Znamy szczegóły budowy Tarczy Wschód," Gazeta Wyborcza, 27 May 2024, **https://lublin.wyborcza.pl/lublin/7,48724,31007099,tak-ma-wygladac-tarcza-wschod-szef-mon-ujawnia-szczegoly-projektu.html**.

79 Latvia already has decided against the use of anti-personnel mines, arguably because of how Canada, where the treaty banning them was signed, is the Framework Nation for the eFP Battlegroup it hosts.

80 Lukas Milevski, "The Baltic Defence Line," Foreign Policy Research Institute, 2 February 2024, **https://www.fpri.org/article/2024/02/the-baltic-defense-line/**.

81 Ibid. See also Maria Engqvist, "A Railhead Too Far: The Strategic Role of Railroads during Russia's Invasion of Ukraine," Swedish Defence Research Agency [FOI], Stockholm, Sweden, 2023.

82 Watling, The Arms of Warfare, 23.

83 See Alexander Lanoszka and Michael A. Hunzeker, Conventional Deterrence and Landpower in Northeastern Europe (Carlisle, PA: US Army War College Press, 2019): 97-98.

could expose Russian artillery to NATO attacks. Secondly, the Baltic Defence Line could push an invading Russian force to canalise, thereby making it concentrate its mass along particular routes where it could face further attrition. Thirdly, the Baltic Defence Line could limit any breakthrough that Russian ground forces could achieve while allowing more time for reserves and reinforcements to arrive, whether to strengthen the line or to engage in counterattacks that push back an invading force across the frontier.

MDO should inform the development of the Baltic Defence Line and Poland's "Eastern Shield" as bunkers and other fixed points could be equipped with sensors that can illuminate the battlefield at varying ranges and levels of fidelity.[84] Marrying sensor technology with machine learning can augment the efficiency of separating signals from noise and reduce the burden put on human operators to parse an overwhelming amount of data. Bunkers can even be hard-wired to minimise disruption in the EMS domain. Still, the information generated by the sensors must be fed to relevant units as well as various command and control structures so that friendly forces can gain as good of a picture of the battlespace as they possibly can. **Ensuring connectivity and resilience to EW threats is crucial, which necessitates an understanding of Russian EW doctrine**[85] Active sensors and their power supplies are most vulnerable given their own emissions. Having a dense and broad network of sensors may create targeting challenges for the attacker. These needs require significant bandwidth efficient command and control structures that can absorb the information, devise plans and distribute the new information to subordinate units. They also require understanding "how terrain interacts with sensors" since various features can affect the signatures that could be detected.[86] Having a home-field advantage still necessitates understanding the home field.

Another benefit is that a robust system of fortification along the eastern flank can reduce the risk of cognitive overload. A criticism of MDO was that it is unduly optimistic about what technology can achieve. By extension, one can argue that it is also optimistic about what individual soldiers can do at the tactical level. Suffice it to say, tactical leaders at the platoon, company or battalion levels coordinating assets across multiple domains while in direct combat with the enemy have their hands full. Manoeuvre is cognitively intensive at all levels.[87] With the Baltic Defence Line and the Polish Eastern Shield', staffs can worry a bit less about speed and movement and instead focus on organising the decision-making environment.

Finally, if the Baltic Defence Line becomes subject to bombardment or some other form of kinetic action, enemy artillery pieces and aircraft would need to be identified and tracked so that they can be subject to counter-attack. This challenge is inherently multi-domain, especially if it involves the use of friendly aircraft for close air support and interdiction of enemy forces. Such aircraft must know where the active battle area is located and which targets to engage. As Jack Watling highlights, the need for deconfliction would intensify, especially if the Baltic defenders follow Ukraine's example in using unmanned aerial systems (e.g., drones) to substitute for artillery and hold opposing ground forces at risk. Man-portable air defence (MANPAD) and short-range air defence system (SHORAD) operators also have to know when they should refrain from undertaking certain tasks.[88]

Fortifications are not risk-free. Fortifications are expensive and historical cases of purported failure like France's pre-1940 Maginot Line and Israel's pre-1973 Bar-Lev Line have given them a poor reputation. However, these failures should not be exaggerated: the Maginot Line forced the German military to violate Belgian and Luxembourgeois sovereignty in order to bypass its strongest points,

---

84 For its part, Finland has already begun work on a 'smart fence' along the border with Russia. It is equipped with sensors and augmented by drones to improve local situation awareness. See Gerard O'Dwyer, "Finland's 2024 Defense Budget Targets Arms Restocking, Border Security," Defense News, 13 October 2023, **https://www.defensenews.com/global/europe/2023/10/13/finlands-2024-defense-budget-targets-arms-restocking-border-security/**.

85 Accentuating this need is how, throughout the spring of 2024, Russia may have used GPS jamming to disrupt local air traffic navigation in the Baltic region. Konstantin Eggert, "GPS Jamming in the Baltic Region: Is Russia Responsible?" Deutsche Welle, 5 May 2024, **https://www.dw.com/en/gps-jamming-in-the-baltic-region-is-russia-responsible/a-68993942**.

86 Watling, The Arms of the Future, 26.

87 I thank Michael Hunzeker for this point.

88 Watling, The Arms of the Future, 183.

thereby precipitating British intervention. German fortifications in the Second World War such as the Atlantic Wall and the Gustav Line imposed massive costs on Allied forces. Fortification on its own will not suffice in stopping a determined and resourceful invader—hence the need to consider how the Baltic Defence Line connects with other military platforms that could be deployed to its relief. Moreover, the Baltic countries have no plans for fortifying their coasts, arguing correctly that they require other systems better suited for maritime defence. Still, the virtue of aligning the Baltic Defence Line explicitly with an MDO concept is to have a clearer organising framework for thinking about how the campaign would proceed and what theory of victory should guide planning.

Elsewhere along the eastern flank local considerations should frame MDO planning. For those countries in the interior of the eastern flank, like the Czech Republic and Hungary, MDO would likely focus more on air defence. MDO, of course, still matters for allied operations, as in the case of NATO's multinational battlegroups deployed across the region. As for Bulgaria and Romania, the Black Sea is its own operational space that demands at least the coordination of naval and aerial assets as well as coastal and air defences. An MDO approach is essential not only for connecting those platforms but also for managing friendly kill chains and disrupting enemy ones. An instructive case is how Ukraine has been able to sink a large portion of Russia's Black Sea Fleet. **A naïve observer might think that a coastal defence system or an unmanned underwater vehicle (i.e. maritime drone) operator identified a surface vessel, tracked it and deployed a weapon against it. In practice, the kill chain is extensive and involves multiple teams—civilian and military—tightly coordinating with one another amid a larger chain of command, with different groups taking on different tasks that relate to target identification, deception and the attack itself.**[89]

89 Interview with former senior Ukrainian military official, 26 March 2024.

4. Recommendations

Nine recommendations arise from the analysis regarding MDO and its application to the eastern flank.

1. The Alliance Must Ensure a Common Understanding of Multi-Domain Operations

NATO has agreed to adopt MDO for coordinating military and civilian efforts in the air, land, sea, cyber and space domains. However, official documents on MDO are often filled with vague buzzwords, allowing stakeholders to interpret key terms in ways that align with their own interests.[90] Since MDO has not significantly influenced defence thinking along the eastern flank, the Alliance has a unique opportunity to foster a shared understanding of this important concept. This would help harmonize doctrinal differences among its older members and address the lack of use and familiarity among its newer ones.

2. Multi-Domain Operations are Much More than Command and Control

A common misconception regarding MDO is that it is largely about command and control. While MDO enhances battlespace awareness on the part of command structures and ensures timely and secure information travels along the chain of command, connectivity is just one key facet. Different combat arms need to work together in ways that transcend their service parochialism and bureaucratic culture. MDO aims not only to eradicate such barriers but also to actively integrate diverse skill sets. Naval units cannot simply be comfortable with shooting at naval units, ground units at opposing ground units, and so forth. Moreover, automation does not obviate human judgment—to the contrary, human operators must still make decisions about the interpretation, sharing and use of data within and across domains. MDO may very well require a deep cultural change to overcome inter-service rivalries and other organisational barriers to data management, sharing and employment.

3. Breaking Service Silos: Military Culture Must Transform

Culture is notoriously difficult to transform. One way to facilitate a change of attitude is through professional military education, especially at the general and staff levels. Some analysts argue that military training, at least in the United States, is too centred on individual branch services. As a result, joint operations, including MDO, fall short of expectations.[91] Military education

90 Allied Command Transformation, "Multi-Domain Operations in NATO – Explained," NATO, 5 October 2023, **https://www.act.nato.int/article/mdo-in-nato-explained/. See also Ellison and Sweijs, Breaking Patterns**.

91 Eric Dayhuff, "The Human Factor: Rethinking Joint Professional Military Education for a Multi-Domain Future," Wild Blue Yonder, 22 June 2022, **https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/3048425/the-human-factor-rethinking-joint-professional-military-education-for-a-multi-d/**.

across the region, whether at the Baltic Defence College or in national military academies, should impart MDO values and thinking. On the civilian side, civilian leaders also must contribute to meaningful cultural transformation by encouraging organisational practices and norms that reward jointness. That may require some risk, as it could involve compelling some services to centralise certain tasks, potentially challening their tendency to protect their own turf.[92]

4. Strengthening the Kill Chain: Prioritize Connectivity to Facilitate Operations

As a concept, MDO can be intimidating since working within just one military domain is tricky enough. The fact that different services and countries have their own interpretations of MDO only adds to the complexity. Although NATO absolutely has the potential to set regulations and standards, especially in the European defence context,[93] its ability to produce a universal understanding of MDO across the entire Alliance is easy to exaggerate.

To mitigate the sense of bewilderment that might accompany MDO, defence establishments should at the very least think in terms of connectivity. Specifically, they should be concerned with how different platforms—within militaries and across them—can link to one another in terms of widening and tightening the kill chain. In the Baltic countries, this means integrating various components of defence and deterrence, such as the eFP (or the Multinational Brigades), the Baltic Air Defence mission, the planned Baltic Defence Line and their own national units. In Southeastern Europe, Bulgaria and Romania should note that Ukraine, in sinking a large portion of the Black Sea Fleet, has had to develop and maintain extensive kill chains that require fusing information across multiple military units and government bodies.

5. Connect to Protect: Sensor Technology Must Be Integrated Throughout the Baltic Defence Line and Poland's 'Eastern Shield'

People live on land and only ground forces can hold and occupy territory. The Russo-Ukrainian War has demonstrated the military value of fortifications by increasing the costs to both sides for undertaking assaults. Yet, fortifications alone cannot repel an invasion, a fact that France's Maginot Line and Israel's Bar Lev Line lay bare. Defensive operations require the involvement of different combat arms, so military units from various services and, in the NATO context, countries must understand what is happening and coordinate with one another to defeat the enemy

92 Interview with former senior Ukrainian military official, 26 March 2024.
93 "GLOBSEC's Private-Public Sector Dialogue #2: The Future of Multidomain Operations," GLOBSEC, 13 November 2023, **https://www.globsec.org/what-we-do/events/globsecs-private-public-sector-dialogue-2-future-multidomain-operations**.

as quickly and efficiently as possible. Indeed, the integrity of the Baltic Defence Line and Poland's "Eastern Shield" may provide the crucial basis for a theory of victory that critics allege is absent in MDO.

Extensive sensor technology will need to be incorporated across any network of fortifications built along Poland and the Baltic countries' eastern frontiers. Data collected by those sensors would need to be linked to various command and control structures as well as to frontline units and their follow-on forces. Moreover, the planned fortifications must integrate with existing allied efforts, namely the Baltic Air Policing mission and the enhanced Forward Presence. Since the project remains in its very early stages, defence planners should consider how the Baltic Defence Line and the "Eastern Shield" would work alongside those measures.

6. Learn from the "Land Down Under": Dominate the Skies and Shores

Russia's brutal full-scale invasion of Ukraine in 2022 has prompted various Eastern Flank countries to expand their investments in coastal and air defence systems. Some national defence establishments, such as Poland with its air defense initiatives, are considering MDO concepts. Most national defence establishments do not, at least not openly and formally as their official documents can testify. However, an MDO approach is essential.

Australia's experience offers valuable lessons for the region, with the caveat that its military is much smaller personnel-wise than Poland but larger than most other eastern flank militaries.[94] Arguably, Australia has successfully implemented MDO in its approach to air and missile defence. It began devising a Joint Air Battle Management that integrated ground-based radars to enhance situational awareness and guide aircrafts to specific locations for targeted purposes. They started enhancing their air defense systems to make them integrated and capable of countering various types of threats. Electronic warfare, ground, and cyber capabilities would complement the system, while guided-missile destroyer-type ships would enhance air defense operations.[95]

Countries upgrading their coastal defences—such as Bulgaria, Estonia, Latvia, Poland, and Romania, — should consider a step-by-step MDO approach. Starting with smaller incremental capabilities and progressively adding assets across different domains will help them address a wide spectrum of threats. By gradually adopting MDO in this manner, the Baltic countries involved

94 Australia's 2020 Defence Strategic Update stated that "Investments are planned in joint command, control and communications systems, joint electronic warfare and defensive cyberspace operations." Department of Defence, 2020 Defence Strategic Update, Australian Government, 2020.

95 See "Joint Air Battle Management System," Australian Government, February 2024, **https://www.defence.gov.au/defence-activities/projects/joint-air-battle-management-system**.

in the Baltic Defence Line need not be discouraged by the significant military technological gap that some eastern flank militaries may perceive in comparison to their more powerful allies.

7. Stress-Test the Network: Push Connectivity to its Limits through Military Exercises

One reason why the Baltic Defence Line is valuable for thinking about MDO is that it offers an organizing framework for connectivity while keeping victory in mind. It trains the mind on a specific problem: the durability of the Baltic Defence Line itself in a scenario involving a ground invasion. Of course, a land assault from an eastern direction is not the only possible vector of attack. It is but one scenario.

Scenarios are practical because they increase the likelihood of everyone agreeing on a certain vision of the problem. More pointedly, a military exercise or war game organised around a particular problem can identify instances when friendly units have trouble communicating with one another, cannot share data or experiences across domains and units due to disruption from EW. Europe's geographical constraints limit extensive MDO exercises, but Latvia's planned new training ground in Selonia may offer a unique opportunity for applying MDO at the outset in its design considering its isolation from large population centres.

Hard and tough exercises are necessary for identifying what needs to be done, but defence establishments must overcome their reluctance to exercise for fear of exposing weakness. Failure does not negatively affect progress. Indeed, exercising to failure is essential to reveal and address weaknesses. Therefore, a subsidiary recommendation is that political and military leaders should promote a mindset that views failure as a learning opportunity rather than as a setback.

8. Mission-Driven Acquisition: Focus Procurement on the Mission, Not the Platform

Many defence establishments tend to focus their procurement and acquisition efforts on specific platforms. Those platforms may have significant military value, but they can also be expensive, carry with them high opportunity costs and may not have enough available personnel to operate them. For example, Poland has recapitalised its military over the last decade in what was arguably a platform-centric process. Only now is it connecting those platforms so that they can be interoperable with each other.

The Polish case is not at all exceptional. However, the Australian experience is once again instructive for those defence establishments wishing to understand how to embrace connectivity at a much earlier stage.

The process is made easier by the fact that Australia has a unified acquisition group responsible for procurement and acquisition across all branches of the Australian Defence Force.[96] That common acquisition group helps build interoperability because it is focused on the mission (e.g., air defence) rather than on particular platforms, all while avoiding the stove-piping and redundancies that characterise the US military.

An implication here is that private industry could get involved much earlier in the procurement and acquisition process for countries. After defense establishments define the missions around which their armed forces will be organized, they should collaborate with private industry to identify potential technical solutions—whether software or hardware—related to data fusion that are suited to their specific military and geostrategic needs.

9. Learn from Ukraine: Balance Technological Optimism with Industrial Production

MDO hinges on militaries using common frameworks and operating systems across their platforms, while taking advantage of the Internet of Military Things (IoMT) to exchange information more effectively over secure networks. The technical demands for achieving these objectives are already high, though they are within reach given advances in ICT. Good reasons exist to be optimistic about what can be done, even if more connectivity and data fusion will still place big demands on how much coordination military establishments can really achieve.[97]

Ukraine's defence against Russian military aggression remains a vivid, if bitter, reminder that industrial warfare requires significant industrial production. Russia depends on its artillery to make territorial gains. In early 2024, Russia was able to make some advances against Ukraine because it made up for its own shortages by receiving large amounts of ammunition and missiles from Iran and North Korea just when the United States was domestically hamstrung from providing more assistance. MDO becomes irrelevant if under-investment and a lack of production leave countries quickly outgunned and depleted. Connectivity across domains is critical to the effectiveness of any military mission in the contemporary era, but military supplies are of existential importance.

96 "Capability Acquisition and Sustainment Group," Australian Government, undated, **https://www.defence.gov.au/about/who-we-are/organisation-structure/capability-acquisition-sustainment-group**.
97 Lindsay, "The Economic Complements."


GLOBSEC
IDEAS SHAPING THE WORLD

GLOBSEC
IDEAS SHAPING THE WORLD

Vajnorská 100/B
831 04 Bratislava
Slovak Republic

+421 2 321 378 00
info@globsec.org

www.globsec.org