The Hague Centre
for Strategic Studies

Empty Promises?

A year inside the world of Multi-Domain Operations

Davis Ellison & Tim Sweijs

January 2024

Empty Promises?

A year inside the world of Multi-Domain Operations

The U.S. Department of Defense's 2023 *Military and Security Developments Involving the People's Republic of China* report noted a 2021 "core military concept" in China centered on multi-domain precision warfare. The concept is "intended to leverage a [Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance] network that incorporates advances in big data and artificial intelligence to rapidly identify key vulnerabilities in the U.S. operational system and then combine joint forces across domains to launch precision strikes against those vulnerabilities."

Sound familiar? It should. It is nearly an exact mirror image of multi-domain operations, the warfighting concept initially developed by the U.S. Army since at least 2015 that has since been copied across NATO. Despite its faddishness, or perhaps because of it, the multi-domain operations concept is now guiding the transformation and modernization of Western armed forces and of their peers. Yet, there are real concerns about whether multi-domain operations will mature into a fully functional warfighting concept or whether it will go by the wayside like effect-based operations in the past.

For nearly a year, we visited some of the main centers for thinking on multi-domain operations. We sat with planners in the Pentagon, officers in the German and Dutch army headquarters, strategists from the Israel Defense Forces, and experts and operators from France, Denmark, and NATO. One of us even worked on the NATO concept once upon a time. We appraised the state of multi-domain operations development with a primary question in mind: Will it actually help to win wars? If so, how?

What we found is that there are few clear answers to these questions. New concepts are often highly optimistic, uncoordinated with other services and allies, and lack any clear theory of success. A warfighting concept is a description in general terms of the application of military art and science within a defined set of parameters. For many contemporary concepts, what has stood out is a mish-mash of ideas, visions, and terms that often have little to do with one another. For some, multi-domain operations is just another step in another revolution in military affairs, with images of missiles and satellites and networks all linked up to destroy an enemy. For others, it is a call for new energy to be put into whole-of-government style integration that can deter everything, everywhere, all of the time.

Far more important is the impact this thinking has on the battlefield. Ukrainian forces in the field have been forced to toss out the maneuver-centric concepts taught to them by their NATO trainers as they have fought to overcome Russian defensive lines. Israeli forces were caught out by a massive surprise attack by Hamas, despite Gaza being perhaps the most heavily surveilled area on the planet, and the war in Gaza has already ground into intense urban combat, contrary to the expectations of the Israeli multi-domain concept. Claims to be able to see all, move quickly, and strike anywhere in order to rapidly resolve a conflict with minimum civilian impact are once again being challenged. Maneuver-centered, multi-domain operations style thinking seems to be making empty promises.

All this means that armed services should be prepared to pivot their efforts from the "thinkers" to the "doers" at training centers and better refine the actual feedback mechanisms between new ideas and the needs and realities of battlefield experience. Concept development should be informed by insights distilled from ongoing wars, as well as from exercises and experimentation within joint forces. It should also seek to articulate theories of success against specific adversaries. Finally, the effective implementation of multi-domain operations depends on the availability of mature technologies, in sufficient numbers, deployed by trained and ready forces.

What Makes a Good Warfighting Concept

In the past, warfighting concepts have helped military organizations win wars. The development of combined arms warfare during World War I and the embrace of mechanization ahead of World War II are archetypes of this success. AirLand Battle (Follow-On Forces Attack in NATO parlance), developed in the 1980s as part of the U.S. Army's post-Vietnam transformation, set the conceptual stage for the lopsided Gulf War victory. The centrality of precision-guided airpower across warfighting concepts would seemingly be proved again over Kosovo in 1999.

For the joint warfighting concepts above to be successfully adopted and implemented, a number of factors needed to be in place. A shared understanding across services and allies with aligned incentive structures contributed to the concepts' actual formal adoption. Military officers enlisted the support of civilian leaders. In the cases above, clear threats focused the concepts on actual operational challenges, rather than theoretical ones. This then allowed for the articulation of a theory of success that spelled out defeat mechanisms that actually made a testable argument, which then drove exercise programs. The technology was sufficiently mature and available in sufficient numbers.

Our research has revealed a gloomy picture for the state of multi-domain operations development in NATO countries and some of their closest partners. Few of the conditions listed above are in place in the cases we studied, creating real risks that new concepts overpromise, underdeliver, and distract vital attention away from solving concrete strategic and operational challenges.

Babylonian Confusion

Multi-domain operations concept development has lacked clarity and worsened confusion across multinational efforts. Across the cases we studied, there was a wide variation of terms and meanings. "Multi-domain" is followed by a range of terms, chiefly "operations" (Denmark, NATO, and the United States), "integration" (the United Kingdom), "maneuver" (Israel) and "deterrence" (Taiwan). *Multimilieux/multichamps* is the French term, while Germany references *Multidimensionalität*. "Domain" and "dimension" often take on different meanings, with some (Denmark, France, Germany, Israel, and the United States) referring explicitly and only to the five military domains (air, sea, land, cyber, space), while others (the United Kingdom and Taiwan) understand the term more broadly to possibly include other government functions. This gallery of terms becomes even more complex outside of English, where the terms "domain" and "dimension" are sometimes used interchangeably, such as in German and Hebrew.

Even within individual concepts, language and even images confound as much as explain. Take the case of the U.K. Multi-Domain Integration Joint Concept Note, and the image below taken from it.

The concept's working definition of multi-domain integration is:

The posturing of military capabilities in concert with other instruments of national power, allies and partners; configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains and levels of warfare.

So the concept is simultaneously strategic, operational, and tactical, encompasses nearly all state functions, and is highly dependent on exploiting a "window of opportunity." This is classic "buzzword bingo," and actually makes it less easy to understand the concept. Ambiguous and vague language, filled with generalities, is quite likely the result of significant bureaucratic compromise. Form, in other words, trumps substance.

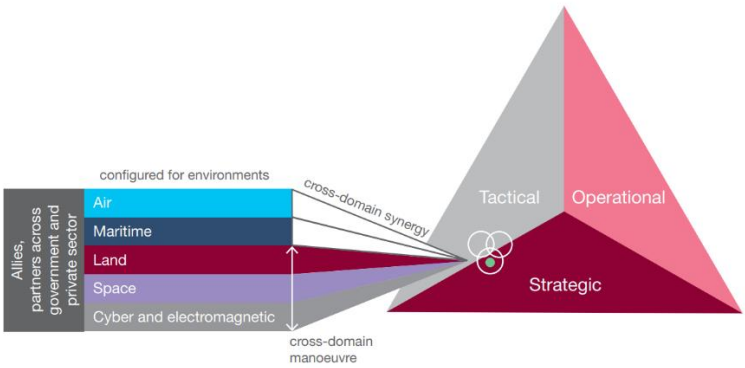

Figure 3.8 – Cross-domain manoeuvre and synergy to exploit the window of opportunity

Figure 1. Image Source

Poor Regime Fit

In many cases, the multi-domain operations concept does not sit well within existing political and military structures. This is particularly the case when a new concept seems to put the military or defence in a leading or coordinating role for other ministries or departments. The British concept, which carries an implicit centrality for the military in a coordination role for all security affairs, has been at odds with the Foreign, Commonwealth, and Development Office and Parliament. The concept is then less digestible within the British political-military system as it proposes an outsized role for defence.

In the U.S. case, inter-service rivalry has been particularly strong and has had a direct impact on efforts to institutionalize multi-domain operations across the whole joint force. The U.S. Army and Air Force led competing development efforts, while the Navy and Marine Corps developed their own service-specific approaches that focused very narrowly on the Western Pacific. Importantly, differing service processes in training, budgeting, and procurement hinder joint efforts by locking implementation into service-specific channels.

At the lowest level, within the services themselves, tensions can be found as well. For many countries pursuing multi-domain operations, namely the United States, United Kingdom, Germany, France, and Israel, the army division has been envisaged as the most appropriate echelon within which to locate it. However, this has not been consistent across cases. Both the United States and Israel have multi-domain units (the U.S. Multi-Domain Task Force and the Israeli Ghost unit) that sit at different levels. In the U.S. case it is effectively a series of theatre-level missile brigades (based in both Europe and the Pacific), and in the Israeli case it is an experimental special forces battalion. Who "does" multi-domain operations remains contentious in Israel in keeping with the long-running rivalry within the army between the airborne and armored corps.

There is dissonance between and within each of these three levels. Concepts stressing a "whole-of-government" type approach risk civil-military tension over command, while those that emphasize precision-strike systems risk inter-service rivalries over who owns these new capabilities or who leads in command. And while these are, largely, peacetime debates, tensions have persisted in wartime, making them all the more crucial to understand.

Technological Immaturity

Much of the technological emphasis in multi-domain operations concepts is on speed: speed in communication, speed in action, and speed in movement. From a certain perspective, positing that war can be resolved early and quickly, this makes perfect sense. Another view, however, is that constantly pushing for speed ignores *tempo*, and that operations can spin out of control of both commanders and political leaders. Additionally, linking tactical and operational speed to strategic outcomes is itself an unproven assumption. Alongside this is the simple material fact that many of these game-changing capabilities just are not there yet. This is especially true for European forces that continue to face significant shortages in these capabilities.

Most concepts fall prey to this technological overconfidence, particularly in the field of communications. Assured connectivity in combat is central to nearly all multi-domain operations work. The United States, United Kingdom, France, Germany, Israel, Taiwan, and NATO all place some style of next-generation command, control, communications, computers, intelligence, surveillance, and reconnaissance capabilities at the core of their concept, assuming an assured availability of strong networks in the relatively near future. In reality, and despite a significant amount of attention in recent years, the level of assured connectivity upon which much multi-domain operations thought is predicated is far from realistic. Given that Russian, Chinese, and Iranian forces have invested heavily in electronic warfare capabilities and degrading their opponent's battlefield connectivity over the past decades, this remains a blind spot. That a significant amount of conceptual and even higher strategic-level work is being done on the assumption of technological maturity is a serious flaw in the current generation of efforts.

There is little reason to assume that the speed and decisiveness imagined by multi-domain operations concepts is technologically feasible or leads to the outcomes desired. High-level efforts in recent years such as the U.S. Joint All-Domain Command and Control system have yet to take major steps. This hubris poses a risk that continues to pervade thinking on the Western way of warfare.

Vague Threats

It seems self-evident that a military concept should designate a specific adversary. If the envisaged result is to compel an enemy to do your will, it makes sense that the adversary and the threat it poses is explicitly taken into account. Many concepts, however, fail to single out adversaries and offer only the vaguest threat descriptions. Though the United Kingdom, France, Germany, and Denmark are *implicitly* focused on Russia and NATO's eastern front, this does not translate into detailed threat descriptions based on enemy approaches. NATO itself is aided in its specificity in that the alliance, through its 2022 Strategic Concept, has two threats that it has agreed to identify: Russia and terrorist organizations. For the United States this is arguably more challenging as its efforts must span global interests. The U.S. Army's multi-domain operations concept is implicitly designed around both a Baltic and Taiwan scenario, implicitly identifying the main problem as ensuring manoeuvrability in a missile-dominated environment.

For countries that still face very direct threats at their borders, such as Israel, Taiwan, or South Korea, this is not a problem. Their concepts identify adversaries and contain clear threat descriptions. The major NATO states do not, which poses a problem from both a strategy-making and defence-planning perspective.

No Theory of Success

Very few of the countries explicitly formulate a theory of success. Only France, Israel, and Taiwan make a tentative causal case for how the new approaches envisioned within their respective multi-domain operations concepts will lead to defeating an opponent.

In practice, such an argument could look like: "IF NATO forces adopt a multi-domain operations approach that incorporates long-range precision fires alongside forward defensive systems, THEN these forces can effectively defeat a Russian attack along the eastern front, BECAUSE these divisions can effectively target rear-echelon targets while blunting assaults by frontline Russian units."

What appears in the hypothetical above is a defeat mechanism. Described by Eado Hecht, a leading Israeli military analyst, these mechanisms describe the various processes that *cause* the damage that is intended to defeat an enemy. Such a mechanism can be rigorously tested, falsified, and refined at training centers.

Naturally, any fully developed theory is imperfect. There is nothing guaranteeing that the NATO example above would work (and in Ukraine, evidence suggests it wouldn't). However, it can be tested in joint exercises, tried in simulations, and measured against observations from contemporary conflicts so that it can be improved and reapplied.

Opaque Risks

A key element that is often missed in new warfighting concepts, and indeed in many assessments of them, is the inherent risk in adopting a new approach. Each new concept involves implicit trade-offs that carry risks. By prioritizing one or another threat, selecting specific capabilities, or proposing new organizational structures, choices are made whose drawbacks are rarely made explicit. At present, none of the cases we studied assesses risks in the way described above. If risk is noted, it is only to argue for the risks if the respective concept is not implemented and funded, a calculation as influenced by bureaucratic considerations as it is by threat perceptions.

There are at least four risks that stem from an uncritical approach to developing multi-domain operation-type concepts: the possibility for commanders to become overloaded by an overly broad span of control; an over-reliance on connectivity; a mechanistic, over-engineered approach that becomes top heavy; and the assumption that the whole is ultimately more than the sum of its parts. Each has and will continue to derail new work if unaddressed.

The Way Ahead

Spending a year with multi-domain operations operators and strategists, we fear that it risks remaining a fashionable idea that is not implemented at scale. The "why" but especially the "how" of multi-domain operations simply does not have a clear or entirely convincing argument. This is not to say it is impossible to improve prevailing concepts going forward, but the current trajectory is not promising. With this in mind, we offer several recommendations.

First, shift from what Buzz Philips calls the "thinkers" to the "doers," without severing the ties. It is almost impossible to test, invalidate, and revisit ideas if they are not being experimented with. For multi-domain operations to progress, it needs to leave the staff office and go to the training center.

Second, stop trying to make war "not war" by being overly clever. New concepts cannot erase attrition from the battlefield or lift the fog of war. Attempts to do so are quixotic at best. Focus on concrete operational problems and build solutions from there.

Third, be specific about adversaries and articulate how multi-domain operations can help defeat them. Task strategists to formulate defeat mechanisms that make clear, causal claims about how a new idea will resolve a tangible military problem posed by enemy forces. Practice these in wargames, simulations, and exercises at the national and the international level.

Fourth, continue to align efforts within NATO and within allies' forces on terms and core ideas. New concepts, particularly for smaller and middle powers, should be multinational by design and language and concepts should be aligned.

Finally, consider the availability of the technologies that are at the core of visions of multi-domain operations. Draw up roadmaps for these technologies with direct links to different force mixtures. Recognize that capacity is just as much if not more important than qualitative capability. Quantity is a quality. Mass cannot be effectively substituted, certainly not in wars of attrition.

In conclusion, are the promises of multi-domain operations empty? Not necessarily. By the criteria identified above, the Chinese approach actually appears quite robust. It has a clear enemy, a theory of success, seemingly clearer inter-service and political-military relations, and is based on existing military capabilities. Regrettably, Western military organizations cannot say the same. They have their work cut out for them to make sure that multi-domain operations delivers on its many promises.

Davis Ellison is a strategic analyst at The Hague Centre for Strategic Studies and a Ph.D. candidate in the King's College London Department of War Studies.

Tim Sweijs is the research director at The Hague Centre for Strategic Studies and a senior research fellow at the Netherlands' War Studies Research Centre.