

Lt Col Andrés Mező

REPORT ON JAPCC MULTI-DOMAIN CONFERENCE

DOI: [10.35926/HDR.2020.1.6](https://doi.org/10.35926/HDR.2020.1.6)

“The dodo is extinct because they lost multi-domain capability.”

The JAPCC (Joint Air Power Competence Center) hosted a multinational gathering of distinguished speakers and panellists at the annual Joint Air and Space Power Conference in Essen, Germany. The theme of this year’s conference was ‘Shaping NATO for Multi-Domain Operations of the Future’, discussed in four themed panels.

The concept of Multi-Domain Operations (MDO) has emerged in military thinking in recent years. Although there have been no serious efforts to define it precisely so far, there is already news that the armed forces of some advanced NATO countries are entering the implementation phase.¹

TERMINOLOGY

At the time of writing there is no clear NATO definition of the term MDO.² The NATO terminology database defines only the information technology meaning of the word “domain”. However, it specifies the terms environment and operational environment, which are used by other NATO publications as synonyms for the word “domain”. Such an interpretation of the word is a mistake and misunderstanding of the notion. A closer reading and analysis of the definition of the term operational environment proves that the environment and the operational environment

Environment: The surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans, and their interrelations.

Operational environment: A composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander.

cover sea, land, air, space, enemy forces, neutral and friendly forces, populations, governmental, non-governmental, international organizations, weather, terrain, electronic and chemical defence situation, and information space, etc. The illustration (Figure 1.) shows the

¹ Roblin S. “The US Army’s Experimental ‘Multi-domain’ Units are practicing how to battle Chinese Warships”. *The National Interest*, 11 August 2019. <https://nationalinterest.org/blog/buzz/us-army-s-experimental-“multi-domain”-units-are-practicing-how-to-battle-chinese-warships>, Accessed on 12 August 2019.

² The meeting of the relevant NATO body, the Allied Joint Operational Doctrine Working Group (AJOD WG) took place between 15-17th of October, discussed the terminology, the meeting report will be released later.

difference between environment and domains. Whilst environment contains the cognitive, virtual and physical dimensions, domains exist in each environment.³

This will bring us closer to understanding the concept of multi-domain, that is, a comprehensive understanding of how a commander can use the capabilities available to him in various domains to operate there, in order to make an impact in the same or in another domain. So, part of the operational environment becomes the domain, because that is accessible for military forces and can be used for military operations.

Let us look at how doctrines define the role of the military in their own characteristic domain. Maritime power is derived from the ability of a state or non-state actor to use the freedom of movement provided by the sea to exert diplomatic, economic, or military influence at a time and place of choice. Maritime power has traditionally been employed globally to maintain the freedom of navigation essential to the general economic welfare or survival of states. Conversely, it has been regularly used to disrupt an opponent's sea lines of communication as part of a wider Allied, joint, or combined operation (AJP-3.1, Allied Joint Doctrine for Maritime Operations). Interestingly, we do not find a similar definition in NATO's land operational doctrine. According to Australian land doctrine, however, land power encompasses the employment of an array of land capabilities – from Army and across government – to achieve specified objectives. The Army must always view itself not in terms of simply “winning the land battle”, but as a force capable of exerting land power for strategic effect across the modern spectrum of peace, crisis and war. The term land power also raises the Army's concept of itself above this tactical “win the land battle” and accepts that the generation of effects on land also has strategic impact. It is multidimensional: land power may involve the employment of capabilities from all the domains (land, sea, air, space and cyberspace) to achieve results on land (extracted from Australian Land Doctrine). Air Force refers to the ability to use air capabilities to influence the behaviour of actors and the course of events (AJP-3.3, Allied Joint Doctrine for Air and Space Operations). As we can see, it is only the Australian land doctrine, which mentions that the land-based armed forces do not operate in isolation but focus their efforts from all the domains on the land domain.⁴

Such a poorly defined and therefore ineffective operation and cooperation of NATO forces risks the Alliance's inability to co-ordinate joint operations in all domains. Particularly critical is the neglect of the non-physical (cyber) domain.

Obviously, today even the simplest military operations require a cross-domain interaction. A land operation without air support is no longer conceivable, and certain land capabilities (marines and Special Forces) have long been integrated into the surface and sub-surface elements of naval forces and into air forces. Nevertheless, there is no trace of this multi-domain thinking in any current doctrine.

In the absence of a clear definition of the MDO, NATO could take the advanced concepts of the United States (US) and the unclear terminology therein. “*Operations conducted across multiple domains and contested spaces to overcome an adversary's (or enemy's) strengths by presenting them with several operational and/or tactical dilemmas through*

³ Grest, H. and Heren, H. “What is a Multi-Domain Operation?” In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 2. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

⁴ Parkinson, J. “Is fluidity the key to effective Multi-Domain Operations?” In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 39. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

the combined application of calibrated force posture; employment of multi-domain formations; and convergence of capabilities across domains, environments, and functions in time and spaces to achieve operational and tactical objectives." This definition is bleeding

from many wounds and does not meet the standards of NATO terminology. It is voluminous, contains reference to itself, and excessively narrows the concept, practically defines doctrinal thought, and despite its length does not contain enough specificity to distinguish it from many other similar concepts (e.g.: joint operations, network-based operation). The United States Air Force Command approaches the issue from a command and control perspective, having produced a definition only for Multi-Domain Command and Control (C2). "The coordinated execution of authority and direction to gain, fuse, and exploit information from any source to integrate planning and synchronize execution of Multi-Domain Operations in time, space and purpose to meet the commander's objectives." From the definition it can be concluded that the MDO differs from the previous concept of Allied Joint Operations. Indeed, the definition of Allied Joint Operations does not explicitly require the forces participating in the operations to cooperate closely. The MDO, on the other hand, goes far beyond this point and requires the military to cooperate beyond operational planning to combine combat effects. The extent to which the MDO concept goes beyond current joint operations is an open question at this time. MDO means mutual support in the traditional operational environment of traditional military forces (land, sea, air) and enters into new domains, such as cyberspace and space.

Studying the doctrines in AJP-3.20 we can find a domain definition. "A discrete sphere of military activity within which tactical actions are orchestrated to achieve objectives in support of the mission. They provide a structural framework for military operations and wider defence activity. They may be integrated but have no hierarchy. While the activity is discrete the consequences and effects are interconnected." On the basis of the above definition, NATO's proposed definition (in text box) was submitted to the Allied Joint Operational Doctrine Working Group (AJODWG). The United States (US) TRADOC headquarters adds to this definition a list of the domains: land, air, sea, space, and cyberspace through the electromagnetic spectrum.

Of the five domains, the cyber domain is prominent, since it connects the other four. Only through networked information technology devices can the commander understand the evolved air, sea, land and space situation, and can process, interpret, control and influence the platforms in other domains.

There are also opinions to extend the concept of a domain to a sixth space, such as the "independent sphere of military activity", which is the cognitive (information, psychological, human, communication) domain. It is argued whether recent counter-insurgency operations have proved that the operations must first and foremost win the support of the population and that not even the most pressing

Multinational joint operation:

An operation carried out by forces of two or more nations, in which elements of at least two services participate.

Domain: A discrete sphere of military activity within which tactical actions are orchestrated to achieve objectives in support of the mission. (Terminology Tracking Form No 2018-0276)

Multi-Domain Operations (MDO)

"An operation to conduct activities and generate effects across more than one domain, at the same time in an integrated manner". (TTF-2019-0229)

firepower can prevent the insurgents from delivering their messages (narratives of actual war events) faster and more effectively. Indeed, on many occasions, news of extraordinary collateral damage first appeared in the insurgents' narrative in the world press, and the official NATO announcement, the refutation, came only weeks or months later, when both world and local public opinion were convinced that NATO soldiers committed murders. The MDO must be viable and applicable not only in high-intensity, symmetric warfare, but also in low-intensity, asymmetric conditions. Opponents of the Sixth Domain, on the other hand, argue that the cognitive is heavily subordinated to the cyber domain, since information is from that domain and they consider the cognitive a dimension rather than a domain.⁵

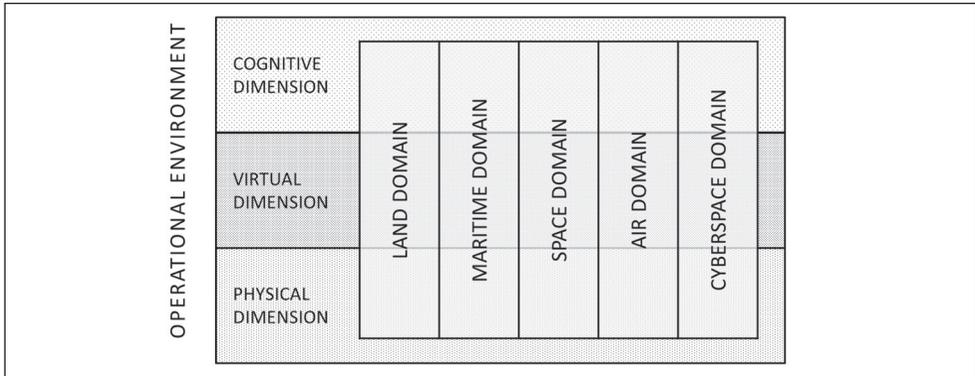


Figure 1 *The five domains in the three dimensions*⁶

The figure above points out that the three dimensions (physical, virtual and cognitive) are overarching the five domains. The “old style” battles concentrated effort mostly in physical domains (land, maritime, air) and dimensions, meanwhile the “new school” has to address all the domains and all the dimensions simultaneously.

HISTORY

These domains, have always existed, even the ancient warlords were already doing multi-domain operations, coordinating the manoeuvre of their ground troops with naval manoeuvres. The disastrous Athenian campaign to conquer Sicily during the Peloponnesian War provides just one example. In 414 BC during the siege of Syracuse, the Spartan strategist Gylippus turned the tide of battle in favour of the Syracusan forces. Gylippus focused initially on the human and political factors, inspiring the Syracusan forces and galvanizing the support of their allies. He then embarked upon simultaneous attacks of the Athenian troops on the land and at sea. By 413 BC, the Athenians had been defeated.⁷

⁵ Canovas, J. “Multi-Domain Operations and Challenges to Air Power”. In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 48. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

⁶ Duchaine, P. “NATO’s challenges in Multi-Domain aka Full Spectrum Operations, presentation.”

⁷ Reilly, J. M. “Multi-Domain Operations”. In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 16-17. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

Did the air count as a domain in this campaign? Or was subsurface water a domain in this case? Certainly not, since Gylippus could not manoeuvre in the air or under the sea and could not achieve any effect in them. Why and when does an existing physical space (air) become a domain? When the first aircraft entered service, it became immediately clear that aviation as a capability was essential for freedom of movement and therefore it was imperative to gain air superiority. In the same way, the deployment of submarines changed the nature of two-dimensional naval warfare into three dimensional. This also leads to a practical definition of the domain: "The critical macro space to which access and control is vital for freedom of operations and therefore superiority therein must be achieved." As the first sputnik was launched, space became the fourth domain. And since the introduction of networked information technology in the military, it has become clear that cyberspace is the fifth one.

The discovery of new domains of warfare has certainly brought the need for unified control of manoeuvre in the various domains. While in the Korean War it was enough to break down force cooperation into days and hours, the concept of Air-land Battle, which was created in the 1980s, required minutes of precision in collaboration between the domains. The MDO requires that sensors transmit data in seconds and that a strike from one domain to another occurs within a fraction of a second.

CHALLENGES

Potential future adversaries of NATO have developed technologies, strategies, and operational doctrines that allow them to fight asymmetrically against the Alliance's military superiority and create a strategic deadlock with attacks from different domains.

The revolutionary disruptive technologies causing the stalemate include newly developed devices, such as ballistic and supersonic missiles, stealth cruise missiles, unmanned aerial vehicles that can be bought commercially and not only for observation and detection, but also for delivering strikes. Continuing the line is high-energy microwave weapons and nuclear weapons that destroy all electrical equipment in a district, without leaving significant radiation behind. In addition, the latter weapon can produce effects in two domains at the same time: blasting a 1 kT nuclear weapon 400 km above the surface could significantly damage or permanently destroy unprotected electrical devices and disrupt the power grids and satellites in space. In parallel with these developments, the potential adversary can enhance the protection of his own air defence systems against electronic suppression by using passive sensors.⁸

China is making huge efforts to control cyberspace. A decisive Chinese superiority gained in this domain would mean that NATO could not see and hear, and would lose its ability to control its weapon systems in a timely and accurate manner. Consequently, initiative will be lost and ultimately NATO's superiority in all other domains would be neutralized.

The domains are interrelated and the effect created in one will definitely have an effect in the other domains. For example, if the opponent intercepted or interfered with the frequencies used to control the satellites, destroyed the ground station controlling satellite, or blinded the satellite itself with concentrated energy beam, it would have a serious impact on the fight in other domains. Plenty of naval and land based communication and navigation systems, weapons systems would be paralyzed, the capacity of satellite detection and early

⁸ Reilly. "Multi-Domain Operations". 18.

warning systems would disappear, complete weapon systems would get unserviceable without accurate positioning. Ships, airplanes and entire land units would lose orientation, the ability of accurate knowledge of each other's position, ability to effectively fire, and even command and control. Commanders will be forced to manage their subordinates in a "mission command" manner, with little or no feedback from the subordinates.

With the spread of the technology needed to dominate cyber domain, the Alliance finds it increasingly difficult to maintain its dominance in this domain. Many are already questioning whether the Alliance would be able to sustain cyber space superiority permanently and universally. Such an expansion of the capabilities of potential adversaries will change the nature of warfare.

REQUIREMENTS

Such a dramatic change in the operational environment places many demands on NATO to meet new challenges and succeed in fighting (or deterring) near peer enemy forces.

- The first requirement is a new, higher level implementation of the oft-mentioned mission command. In the future operating environment NATO will have no superiority in the electromagnetic spectrum, and communications and IT networks will become unreliable. Commanders have to upgrade the "centralized decision-making, decentralized implementation" to "distributed control, decentralized implementation." The details of this type of C2 are not clear at this moment.⁹
- Commanders must be familiar with the idea that in the future theatre of operation they will have no more comfortable superiority in any of the domains. The loss of aerial and electronic superiority will be extremely sensitive to NATO forces, because they did not have to face such a challenge in the past 60 years, since the Korean War.
- The third requirement is the elimination of the so-called independent (stovepipe) service thinking. The new concept should be based on the interconnection of the five operational domains, their mutual support, and the operational effects among the domains. The effects achieved in each domain must support those in other domains, and create synergies in a complex, all-domain environment. The supporting and supported relationship will change constantly as agile commanders execute strikes from one domain into another. The decisive strike will not occur in one or in another domain, but almost simultaneously in all domains.¹⁰
- The fourth requirement is that it is not enough for NATO to win the war, but it has to be prepared to win the peace. Moreover, ideally, like the in the Cold War, there will be no armed conflict between NATO and near-peer armies, but NATO's preparedness itself will be sufficient to deter the war. Armies are capable of winning battles and campaigns, but only a committed, whole-of-government policy can win both the war and peace. Isolated military results without other aspects of national power of the member states are not capable of winning the competition against Russia or China.
- The fifth requirement is to find the opportunity for NATO to have proportionate capabilities in all the five domains. While NATO has significant capabilities in physical domains,

⁹ Reilly. "Multi-Domain Operations". 22.

¹⁰ Carlisle, H. J. "The complexity of the Multi-Domain Operations". In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 33-37. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

NATO's cyber and space capabilities are currently based solely on voluntary contributions from member nations. Most of the Member States do not have any offensive cyber capabilities at all. The problem does not only arise in the field of capability development. The use of space and cyberspace for military purposes raises enormous legal concerns as well. Unless these are addressed and satisfactorily resolved, we risk yielding the two domains that link the other three, thus making our capabilities isolated and easy to counter. However, the use of these two key domains is not a legal challenge for Russia and China. Collective cyber-defence (including cyber-attacks) is currently prohibited under positive international law.¹¹ The dominance of space and cyberspace will be vital to NATO, the superiority gained in these two domains does not necessarily mean victory over the other three spaces, but their loss is certainly a defeat.

- The biggest challenge of MDO is to bring together the five domains, to develop an operation control system that not only integrates service-based operations centres, but also enables the commander to visualize operations and make quick decisions.

OPPORTUNITIES

John Boyd's OODA cycle (Observe, Orient, Decide, and Act) helps develop the C2 governance system. The idea is that a Multi-Domain Operations Centre (MDOC) consists of three layers. The first is perception (reconnaissance and intelligence), which allows the commander to understand the operational environment, and to explore the relationships among domains, the second one is the command and control layer. The commander must be mindful of the varying operational tempo and significance of the domains, the light infantry and special operations forces are capable of traveling at 3-4 km, the mechanized, airborne and naval forces reach their destination much faster, the air force is moving at the speed of sound, cyber operations are practically at the speed of light. MDOCs should coordinate multi-domain operations so that they exert their effects almost simultaneously, thereby achieving a complex effect that prevents the enemy from responding adequately. The dominance of cyber and electromagnetic domains is of paramount importance. Without protecting our own networks, NATO forces become out of control, and by gaining and establishing superiority in these two domains, we can deprive the enemy of perceiving and communicating. Finally comes the effect layer, which includes battlefield systems that generate kinetic and non-kinetic as well as information effects.¹²

Here is a possible scenario for demonstrating multi-domain operations. Internet attacks and operations with electronic jamming equipment (cyber domain) have successfully paralyzed the enemy's integrated air defence system, allowing NATO's reconnaissance aircraft (air domain) to fly over and detect enemy strategic targets. According to the information transmitted, the MDOC directs a submarine fire a Tomahawk missile (sea domain) onto the enemy satellite command centre (space domain) in order to paralyse its communication and real time satellite reconnaissance system. The MDOC simultaneously launches an amphibious operation (land domain), taking possession of the enemy's commercial port, thereby cutting off his economic influence.

¹¹ Väljataga, A. "Tracing opinio juris in National Cyber Security Strategy Documents." In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 91-97. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

¹² Carlisle. "The complexity of the Multi-Domain Operations". 35.

In the example above, each operation initiated from a domain exerts a decisive effect in another domain, and thereby prepares the next operation. The tempo and co-ordination of operations deprive the enemy of his vital skills almost simultaneously and present him with so many problems mutually reinforcing each other's influence that the enemy is unable to prepare and respond adequately.

The current joint force C2 systems are not appropriate for such an operational tempo. What we call joint operations today are in reality nothing more than the coordination of single-domain operations, timing their successive sequences without even attempting to exploit cross-domain strikes in order to mutually support each other. Authority is delegated to the lowest operationally competent level possible, in order to prepare future battlefield commanders to command by mission orders, leave their subordinate commanders to decide within their specified limits and constraints, and leave them to plan and execute cross-domain strikes.¹³

The new dimension of mission command leadership is called distributed control, and this is how MDC2 was defined. Distributed control and decentralized implementation allow for shorter chain of command, faster decision making, and significant C2 benefits. At this moment, we have neither definition of distributed control nor description the concept of it.

Multi-Domain Command and Control (MDC2): Command and control that directs and enables the simultaneous conduct of multiple operations across more than one domain in an integrated manner.

The key to MDOC2 is connecting and sharing information at the highest possible speed in real time. C2 relies on a cloud-based database into which all information collected by sensors from each domain is uploaded. This allows a reduction of the time needed for targeting and delivering strikes. In the complex process of targeting, automated and IT-supported processes immediately determine what action the Rules of Engagement allow. They also determine what collateral damage (?) and what primary and secondary effects are expected, and in which domain (or domains) which weapon systems are best suited to attack the target. This allows the commander, in his or her delegated powers, to take advantage of the short time the target is exposed and instantly strike from as many domains as possible and by the most appropriate platforms.

It is important that data are shared as widely as possible and that the electromagnetic spectrum remains secure. This requires NATO to develop new data sharing mechanisms and standards as well as encryption mechanisms for the multi-domain network. There is a lot to do in this regard, as it is not just a technological issue. For nations, sharing information also raises legal and political issues.

The continuous operation of networks requires the networks necessary for MDO to operate not on a server-client basis, but as a peer-to-peer system capable of self-healing. In case of disruption or destruction of certain network elements, other elements of the network take over their role and pass the necessary information to the recipient. The development of technology makes this possible.

The basic principle of information sharing ("need to know") has to be replaced by a new approach, which recognizes that there is much more risk in keeping back information within

¹³ Canovas. "Multi-Domain Operations and Challenges to Air Power". 49.

the Alliance than in potentially unnecessary information sharing. A concept of analysing and interpreting large amounts of data generated in the network needs to be developed. The potential of artificial intelligence for automated data processing and machine learning has to be utilized. The use of these revolutionary disruptive technologies would also be of enormous advantage to our enemies, so we must take immediate action to be able to counteract this advantage first and neutralize this advantage when it appears in the arsenals of China and Russia.¹⁴

Science provides an inexhaustible range of combat capabilities. It is no longer a dream to have a machine-to-human interface. In the future, commanders will be able to control many command and weapon systems at the same time simply by brains or eyes.

Staying on track, NATO's MDO training environment will need to be developed in the future. A virtual environment should be created where future MDO theory can be put into practice. There is a need for a computer simulation infrastructure where our MD concepts can be tested. Multiple-level MDO attacks must be simulated, based on the potential real enemy's doctrine. The exercise scenarios have to contain deprivation of superiority in one or more domains. Regaining lost superiority and subsequent decisive strikes must also be exercised. The MDO should be tested not only in high-intensity combat, but also in hybrid warfare, proxy war, anti-insurgency scenarios. Efforts should be made to reflect not only the impact on the enemy during the war, but the activities of a wide range of state (police, militia), international (Red Cross) and non-state actors (ethnic groups, criminals) should be also simulated. Ownership of the space domain is crucial, and such scenarios should be injected into exercises as well.

SUMMARY

Huge efforts are being made by NATO and its member states to prepare for the fight against near-peer forces. The new concept is called multi-domain, and it represents an evolution from the previous joint operation concept. In MDO new disruptive technological tools and procedures are widely used. The conference supported our effort in the given concept development task, we were able to expand the community of interest, and we received inputs about the opportunities to address in the future.

BIBLIOGRAPHY

- Canovas, J. "Multi-Domain Operations and Challenges to Air Power". In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 47-54. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf
- Carlisle, H. J. "The complexity of the Multi-Domain Operations". In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 33-37. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

¹⁴ "Doolittle Series 18 Multi-Domain Operations". In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 70. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

- “Doolittle Series 18 Multi-Domain Operations”. In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 65-71. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf
- Ducheine, P. “NATO’s challenges in Multi-Domain aka Full Spectrum Operations, presentation.”
- Grest, H. and Heren, H. “What is a Multi-Domain Operation?” In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 1-4. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf
- Parkinson, J. “Is fluidity the key to effective Multi-Domain Operations?” In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 39-45. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf
- Reilly, J. M. “Multi-Domain Operations”. In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 15-24. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf
- Roblin S. “The US Army’s Experimental ‘Multi-domain’ Units are practicing how to battle Chinese Warships”. *The National Interest*, 11 August 2019. <https://nationalinterest.org/blog/buzz/us-army-s-experimental-“multi-domain”-units-are-practicing-how-battle-chinese-warships>, Accessed on 12 August 2019.
- Väljataga, A. “Tracing Opinio Juris in National Cyber Security Strategy Documents.” In *Shaping NATO for Multi-Domain Operations of the Future: JAPCC Conference Read Ahead*. Kalkar: Joint Air Power Competence Centre, 2019. 91-97. https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf