Joint Air & Space Power Conference 2019

Shaping NATO for **Multi-Domain Operations** of the Future

CONFERENCE

PROCEEDINGS

Joint Air Power Competence Centre

The JAPCC team thanks you for participating the 2019 Conference.

Disclaimer

The Joint Air Power Competence Centre (JAPCC) Conference Proceedings is a product of the JAPCC. It is produced to provide a summary of the Joint Air & Space Power JAPCC 2019 Conference and subsequent proceedings. It does not represent the opinions or policies of NATO and reflects independent analysis, opinion, and the position of its authors.

Release

This document is approved for public release. Portions of the document may be quoted or reproduced without permission, provided a standard source credit is included.

Published and distributed by

The Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140
47546 Kalkar
Germany

Table of Contents

The JAPCC Conference 2019

Sponsor Recognition

AIRBUS

AIR UNIVERSITY

CUBIC

ELETTRONICA GROUP
Defence I Cyber I Security

GENERAL ATOMICS
AERONAUTICAL

LOCKHEED MARTIN

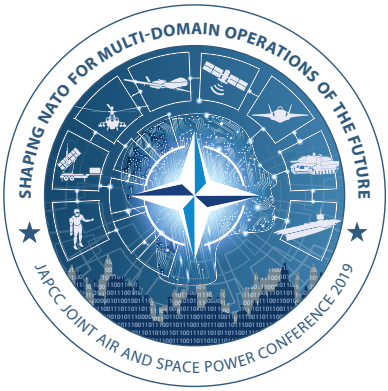
THE VALUE OF PERFORMANCE.
NORTHROP GRUMMAN

SNC SIERRA NEVADA CORPORATION

ThalesRaytheonSystems

The JAPCC wishes to thank all sponsors for their contribution to this year's Conference and for helping to make it a great success.

Klaus Habersetzer
Lieutenant General, DEU AF
Executive Director, JAPCC



This book contains the proceedings of The Joint Air Power Air Power Competence Centre's annual conference held at the Messe Essen, Germany from 8–10 October 2019. The theme for this year's conference was:

'Shaping NATO for Multi-Domain Operations of the Future'

In this edition of the conference proceedings, we have captured and themed the results, rather than publishing a chronological recounting of the panel discussions. We hope this makes it easier for our readers to identify the key takeaways.

We thank those of you who joined us for your contributions to the discussion, and hope that those of you who were unable to be there will find this wrap-up informative and thought-provoking.

If you wish to provide feedback on these proceedings, or the conference on the whole in order to help us increase the value of the event, please send us your feedback at conference@japcc.org.

Thank you and good reading!

The Joint Air Power Competence Centre (JAPCC)

Shaping NATO for Multi-Domain Operations of the Future

Opening Address by General Jeffrey L. Harrigian, Director, Joint Air Power Competence Centre.

Introduction

The JAPCC Conference, held in Essen, Germany from 8–10 October 2019, concerned itself with Multi-Domain Operations (MDO).

This paper aims to capture key messages from the conference. Rather than producing a chronological record of these discussions, it will introduce them thematically. There were several recurring key themes across the two days of the conference. These key themes were clearly ones which concerned and engaged the 344 attendees of this 2019 JAPCC Conference.

The themes identified also lead to some key takeaways. The importance of the subject matter discussed caused several senior speakers to exhort the JAPCC to go beyond merely identifying key takeaways. This paper, therefore, takes the bold step of suggesting quite concrete actions for NATO – via the JAPCC – to take.

For a fuller understanding, readers are encouraged to consider this paper in conjunction with the previously published Conference Read Ahead material. Additionally, in the spirit of the Chatham House Rule, no statements, opinions or ideas are attributed to any particular individual within this paper. This caveat does not apply to the authors of published works referred to within.

The Global Commons

Space and cyberspace – two things that, in recent times, have been referred to as 'global commons' – have quite clearly been shown NOT to be in common ownership. Space-faring nations (as opposed to space-using nations) are aware of this. Control of these so-called global commons can (quite suddenly) be wrested away from any democratic nations who rely solely on goodwill and treaties to protect this common ownership.

No-one should, perhaps, be surprised by this. The World's oceans – outside of nations' territorial waters – are also one of the global commons. However, for several hundred years, maritime nations have accepted that control of the sea (to a greater or lesser degree) is necessary to ensure and assure global trade and overall prosperity. Many nations have invested heavily in navies in order to do this. In the 21st Century, NATO must also take steps to establish and ensure free use and free passage for space and cyberspace users.

Application of MDO to Future Conflict

In addition to the challenge of securing the broadening global commons, NATO is currently faced with both ongoing cyber warfare and 'lawfare'. These elements will present monumental challenges in future conflict. While the next war is always to be avoided, if it occurs, it will be different than anything we have seen in recent decades and leaders must be ready for the new and different problem sets they will face. Pragmatism demands that we must be prepared for disrupted satellite access (particularly position, navigation, and timing), cyber-attacks on critical networks and infrastructure that may not be readily detectable, a contested space domain, and greater cross-domain complexity than ever before. Moreover, some have posited that adversaries have 'stolen the march' on the alliance in terms of electronic warfare and A2AD capabilities, and that NATO's military capability is approaching a sigmoid curve, where its technological advantage has been eroded and is therefore compelled to embrace a new path moving forward.

MDO represents that new path, one that will require connecting, decision-making, and responding at speed. It will require resilient networks and a degree of sharing among allies not yet achieved. It must commence with an entirely new frame of thought, much of which will be fuelled by the younger generation of leaders. Most importantly, it is a challenge that cannot wait for years of development, nor can it be solved in one fell swoop.

Bruce Hargrave, Moderator.

We must begin making incremental steps now and not be afraid to 'fail fast' in the pursuit of progress.

The Read Ahead material for the JAPCC Conference set the scene for an in-depth discussion of MDO. From a US Army perspective, General Townsend's article 'Accelerating Multi-Domain Operations: Evolution of an Idea', traces the MDO concept as having evolved from Multi-Domain Battle (MDB). As General Townsend explains, this original nomenclature led to the criticism that MDB was an Army-only concept. He also asserts that words, and their meanings are very powerful and should not be used lightly or inaccurately. This is a point that will be developed and referred to throughout this paper.

THEME 1: Defining Multi-Domain Operations

Three Little Words

The Conference spent some time – particularly in the first morning's keynote address and panel one – examining the words tied up in MDO and proposing definitions. The first two words are often shown hyphenated – 'Multi-Domain', although this is not always the case. Little problem is encountered with the word 'multi', taken to mean 'many' and to (usually) imply a lot more than one. Military and military-associated people are also familiar with the use of the word 'operations'. It means a level of military activity beyond training and exercising. It does not necessarily imply kinetic warfare (see, for example, Peace Support Operations) but it will include that. In other words, it implies serious stuff – yellow bands on munitions and blank ammunition and drill rounds left at home.

So, perhaps the word 'domain' is the only one that some might struggle with. For many years, NATO has been happy with the traditional idea of components – Land, Maritime and Air – and the way in which they are used to refer to the Army, Navy and Air Force. Additionally, it is generally acknowledged that there are organizations that operate across more than one component – the Marines would be one example. The edges begin to blur more when we consider aircraft operating from the land and the sea and that navies and armies also operate aircraft. In the traditional understanding of the three main components, space and cyberspace were seen as 'key enablers'. However, as components realized the vital (rather than key) nature of these two enablers, space and cyberspace attained their true position as domains, alongside the domains in which the components operate. In summary, at least five domains are now acknowledged – Land, Maritime, Air, Space and Cyberspace.

This is all discussed in greater depth in the Read Ahead article by Dr Donnelly and LCDR Farley – 'Defining the "Domain" in Multi-Domain' (page 7). They explain that 'the notion of an operating environment (OE) is not the

same as a domain' because an OE can cover and include some or all of the domains set out above. Additionally, and as the Conference rightly acknowledged, this is even before we acknowledge the three components of fighting power – moral, physical and (of particular importance when discussing new ideas) the conceptual component. These three components of fighting power form the keystone of the military doctrine of many NATO nations.

There are those who are keen to argue that MDO has been around for years, before it was given a neat three-letter abbreviation – the old wine in new bottles argument. General Townsend's article in the read ahead suggests a logical counter to this argument and conference discussions served to take this further and asked:

If we remain convinced that we cannot quite formulate what MDO exactly is, how will we know when an adversary is using MDO against us?

By deciding on an agreed definition of MDO, NATO can take positive steps towards adjusting its posture so that it can more easily engage in MDO and, just as importantly, defend against an adversary determined to use MDO against NATO.

Lieutenant General Thompson, Vice Commander, US Air Force Space Command.

Until quite recently, NATO did not have a definition of air power – relying instead on some amalgam of doctrinal definitions from the individual member nations. Whilst this has been remedied recently, the same state of affairs cannot be allowed to long endure for such an important concept as MDO.

An early attempt at an MDO definition, by combining ideas from several sources, might look something like:

'MDO are operations where activities are conducted and effects generated simultaneously across more than one domain in an integrated manner.'

However, this can be improved upon (perhaps considerably) by some simple analysis and by considering what effects MDO should achieve. One of the simplest tools for analysis is 'Five Ws and H' or 'Who, What, Why, When, Where and How?'

One of the outcomes from day one of the conference was an answer to many of these Ws and these are set out in the bullet points below:

- **Who** – NATO or the NATO Command Structure.
- **What** – What MDO means is the ability to present multiple simultaneous dilemmas to an adversary, with the aim of overwhelming his decision cycle and getting inside his OODA loop.
- **Why** – Why MDO is important is that waiting to see what happens (or what an adversary does) is unlikely to be a viable option – reacting to multiple dilemmas presented by an adversary will sap NATO's capacity to cause them for the adversary. This represents a dilemma in itself – adopting a purely defensive posture tends to mean that NATO will have to take, absorb and respond to the first 'shot'. In MDO, there is no such thing as a first shot – it is a wave of simultaneous first shots distributed unevenly across multiple domains. There is, therefore, an imperative for NATO to be more proactive and agile.
- **When** – Simultaneously and unpredictably.
- **Where** – Across multiple domains.
- **How** – By using speed, agility and integration – without limits. This tends to imply the use of a certain level of autonomy, and this was characterized (variously) as the difference between human-in-the-loop (HITL) and human-on-the-loop (HOTL). Levels of autonomy are discussed as one of the key elements facilitated by artificial intelligence (AI). AI and Big Data form the basis of one of the themes discussed later.

The results of this analysis can now be combined into an **initial draft definition of MDO**:

MDO is the ability to use information-enabled command structures and combat capabilities, across an array of domains, to present multiple, simultaneous dilemmas to an adversary with the aim of overwhelming him.

This definition, derived after the conference but informed by conference discussions, is one of the key takeaways and implies a follow-on task:

ACTION: The JAPCC Directorate should act as champion for the rapid adoption, by NATO, of an agreed definition of MDO. This definition should be incorporated into NATO doctrine at AAP or AJP level.

THEME 2: Defending Space and Cyberspace

'Winning the battle in space may not lead directly to winning the war. But if you lose in space, you are guaranteed to lose the war'

NATO may need to adopt a more offensive posture to deny adversaries the use of space – 'killing the archer' can be a justifiable means of defending oneself; however, it is still defence and 'you don't win until you start punching back'. The positive message to come out of the conference was that, whilst it had not always been the case in the recent past, NATO no longer has its head in the sand about space.

Twelve months ago, the proceedings for the 2018 JAPCC Conference stated that:

'Likely adversaries have made it clear that they are developing, fielding and expect to operate counter-space weapons. NATO must prepare for physical and cyber-attacks against ground stations and other space mission nodes …'

Air forces have never doubted that their overriding operational mission must be to gain and maintain a requisite level of control of the air. Against a near-peer adversary, this is likely to be a fluid situation where absolute control of the air is not always going to be possible. Will NATO find itself in a similar position where control of space is concerned? If the battle for control of space is a series of consecutive smaller battles, then there is a chance that it will be. If, however, MDO is used to gain control of space then it is likely to be characterized by simultaneous attacks – physical attacks against space hardware and ground stations, cyber-attacks against control systems and data streams, denial of receipt of satellite signals and imagery etc. etc. The effects of such attacks are likely to cause the 'multiple, simultaneous dilemmas' characterized in the proposed definition of MDO. In many (if not most) circumstances, space capabilities cannot be replaced in hours, or even in days.

'Adversaries are using MDO against NATO right now!'

The results and lessons learned over the years from the USAF's annual Shriever Wargame (the 13th such wargame concluded at Maxwell AFB on September 13th 2019) are unequivocal and the conclusions that are drawn vary little year-on-year – even 'a day without space' is likely to severely degrade NATO's ability to operate and to defend itself. In recent years, the phrase 'a day without space' has been expanded to 'a day without space and cyber' and this reflects the growing realization that both of these domains are key. In fact, each one of these domains frequently relies on the other.

'Can we replace a space capability in hours? In days?'

It was also observed that the electromagnetic spectrum (EMS) is vital for all of this. The 'glue' between all of the space, cyber, air, land and maritime capabilities. However, this is an area that has been neglected by NATO

members for more than 2 decades, and now we need to recover the ability to control and dominate it. It was suggested that securing the EMS from attack from potential adversaries is a vital first step. However, if the EMS is analogous to the oxygen that all human life depends on to survive (and it sounds as if it is) then what policies and protocols can be put in place to assure its continued use, free from contamination?

Four key elements are required for successful MDO and these were outlined, in reverse order, as:

- Sustained, reliable logistic support. Something that can never be taken for granted, particularly in a contested environment.
- Effective combat power – but also generating that same combat power in space and cyberspace. In the case of cyberspace, we may not even know what generating combat power within it should look like.
- Superior battle management – with humans on the loop (rather than in the loop – see the later discussion of this) ready to intervene, take new data and rapidly decide on courses of action (CoAs).
- Space superiority is the number one priority. NATO won't necessarily win the war with it, but losing in space virtually guarantees that NATO will lose it.

Somewhat reassuringly, the USAF has been addressing the problem of space superiority for the last 4 years and has made huge progress particularly in the last 12 months. However, the USA is only one of 29 nations that comprise NATO and each of the other 28 must also play their part if the Alliance is to achieve true space superiority. As the commander of US Space Command and Air Force Space Command, General Raymond, stated recently at Maxwell AFB:

'One of our big takeaways … was just how important the coalition is and partners are in space. That provided a great advantage during the game. We've learned a lot every time we've played that game as it relates to our allies. It is clear that we're stronger together. It's also clear that our focus, again, is to deter conflict.'[1]

Major Gibson's article in the Read Ahead (page 73) 'Multi-Domain Operations and Counter-Space' is an excellent place to start for those who wish to read more on this subject. Whilst it may be more US-focussed, Gibson's assertion is that the need to mitigate the A2/AD capabilities of a near-peer adversary was the key driver for the creation of the MDO concept. This is another view to set alongside General Townsend's evolution of the MDO concept from the (potentially) Land-centric concept of multi-domain battle.

Turning now to the second domain within this theme, it was observed that, in cyberspace everything is possible and that each one of us accesses it and is therefore vulnerable via numerous gateways (personal computer, work computer, cell phone, etc.)

Cyberspace is a plastic domain – it can be reconfigured by those who know how. NATO must recruit and build a cyber-infantry that has the knowledge and resources to do this. Federated Mission Networking (FMN) is one step towards this. FMN is a capability that aims to support command and control and decision-making in future operations through improved information-sharing. It provides the agility, flexibility and scalability needed to manage the emerging requirements of any mission environment in future NATO operations. FMN is based on principles that include cost effectiveness and maximum reuse of existing standards and capabilities.

(Note: There is much more information about this on the ACT website.)

Cyber-attacks on vital networks are nothing new. They are happening on a daily basis and yet only make the 'front page' when:

1. They succeed, and
2. We can directly observe their effect.

Lieutenant General Gerhartz, Chief of the German Air Force.

Examples of this would include the 'WannaCry' ransomware / cryptoworm attack on systems running MS Windows. Users – including many NHS hospitals in the UK – were locked out of vital data and were told to pay a ransom in Bitcoin cryptocurrency to unlock their systems. In many cases, poor or non-existent network security protocols increased the severity of the effects from this attack and increased the time required to recover from it.

And yet technology companies deal, again on a daily basis, with cyber-attacks – the vast majority of which do NOT succeed. The key tool in defending against cyber-attack is AI developed from rigorous testing and probing – by 'white hat hackers' (hackers working for the common good as opposed to 'black hat hackers' working with malicious intent) – to determine system weaknesses and vulnerabilities.

In cyber-operations, the network is a weapon system – and it can be just as robust or just as vulnerable as any physical weapon system – depending on how it is managed, used and protected. Sadly, it is still the case that the weakest part of many computer networks remains the network users themselves. IT security experts used to admit that one of the simplest ways to introduce malware into an organization's network was to drop a USB stick containing it in the car park. It then just required a well-meaning employee to plug the USB stick into a networked PC –'to check and see if they can find out who dropped it' – to cause a cybersecurity breach. Fortunately, contemporary network security measures mean that this is far less likely to happen now.

THEME 3: Human Factors and Military Culture

'Technology is the easy part. Human factors are the really difficult part.'

In discussions, one key belief was that MDO is not a concept that can await future development.

– Adversaries are using MDO against NATO right now and several examples on or near NATO's eastern borders where discussed.

If MDO has indeed been around for a while, then why is NATO finding it so hard to deal with or (perhaps) even recognize? This may all come back to effects. If the effect required is to create multiple simultaneous dilemmas for an adversary (and the draft definition presented earlier suggests that it is) then, at the point where NATO finds that it is presented with multiple simultaneous dilemmas, it may be worth considering that MDO is being used against NATO.

The recommendation derived from this is that NATO must consider how to counter the use of MDO by an adversary.

As described earlier in this paper, space and cyberspace used to be seen as enablers rather than domains in their own right. The Air University Press definition of MDO command and control (C2) was used to unpack the problem and to describe it as the 'military expression of the internet of things'.

The conference discussed how, from a naval standpoint, particularly within a carrier air battle group, MDO is sometimes characterized as already being conducted by and within the maritime component (rather than across components). Perhaps there are lessons to be learned here. Whilst it may contradict the whole ethos of MDO to believe that it could reside entirely within one component, a carrier air battle group may provide a suitable microcosm in which to study MDO further and identify lessons that can be applied across all components and domains.

Early conference discussions led to two interesting hypotheses about MDO:

- that MDO was about systems and not platforms and
- that culture change was needed for MDO to really come to fruition (see the discussion on culture and culture change later in this paper).

Two notes of caution were also raised. In NATO's search for the faster decision-making mechanisms needed to enable MDO, it should beware of dispensing with wisdom for the sake of speed. Faster decision-making is not necessarily better decision-making. Particularly for NATO's civilian leaders at the political level, what is needed is increased 'decision space'. It might be that greater decision space could be enabled by the considered use of MDO. In this vision, increased decision space allows for wisdom to propagate through the kill chain, so that wise military decisions are taken rather than simply rapid ones. Moreover, decision speed in a MDO construct could quickly outpace the ability to affix attribution; a concern exceedingly relevant in the cyber domain. 'Decision space' will be vital to ensure the origin and severity of activities within complex cross-domain operations.

Another excellent question that exposed one of the dilemmas of MDO was that of mission command and the downwards delegation of decision-making. The example of GPS jamming and spoofing by Russian warships

in the Eastern Mediterranean – where decision-making on their use was delegated to ship captain level – illustrated an area where a potential adversary may be more comfortable than NATO with delegating operational decision-making so that it can have strategic effect. This real-world example was about how a potential adversary might create multiple simultaneous dilemmas for NATO – by enabling the delegation of decision-making through mission command. It was not clear that NATO had the organizational mindset to either match this or to act in similarly innovative ways.

Monkey First

A question from the conference floor likened NATO's journey towards MDO to a problem given to Google's Moon Shot Division:

They must teach a monkey to recite Shakespeare while balancing on a 20 foot pole. Being engineers, they set to work designing the pole. They spent many hours and consumed much of the funding designing and building a beautiful pole, only to realize that they had no idea how to get a monkey to recite Shakespeare.

This anecdote reminds us that our natural tendency is to attack a problem beginning with the aspects we understand or are comfortable with and frequently results in our ignoring the 'long pole in the tent,' or that portion of the problem which is the most difficult or perhaps even unsolvable given the resources available. By neglecting to accurately assess the problem and address the 'monkey first,' time, productivity, and resources may be squandered. In the opinion of one attendee, the monkey for MDO is a fully networked Air Operations Centre for NATO that operates around the

clock with full connectivity. If NATO cannot solve the technical connectivity piece for the Air domain, then we cannot hope to expand it to network all domains.

Culture and the Need for Culture-Change

Another theme to emerge from the Conference was that of culture and a perceived need for there to be cultural change if MDO is to become a reality. A bit like MDO, 'culture' is a word that, when someone uses it, it's automatically assumed that everyone else knows what he or she is talking about. In other words, it is very rarely defined but instead becomes modified by adding words to it so that it becomes 'military culture' or 'NATO culture'.

These are interesting constructs, but we may struggle to find proof that they actually exist in any homogeneous form. For example, whose military does 'military culture' refer to? Is it the US military? Or the French military? Or perhaps the Turkish? Are they the same? And is 'NATO culture' the same thing in Brussels as it is in Norfolk, Virginia? Is it the same as 'organizational culture'?

This is not an attempt to dismiss the importance of culture, merely a plea for the need to define the term very carefully. Bower's 1966 definition of an organizational culture as 'the way we do things round here'[2] is still relevant today and will have a ring of truth to it for anyone who has operated 'cross-culturally'. Charles Handy (1976) takes us a step further when he describes an organizational culture as the 'deep-set beliefs about the way work should be organized, the way authority should be exercised'[3]. However, anyone who has ever changed squadrons on the same frontline airbase (i.e. gone from flying with x sqn to flying with y sqn) will soon tell you that there also seem to be sub-cultures, even within the same military on the same base. Perhaps these types of sub-cultures have something to do with the stories we tell about ourselves, the patches and badges that we wear and the myths and legends that we create?

Mansoor and Murray, in their 2019 book 'The Culture of Military Organizations', give a broad definition of organizational culture as *'the assumptions, ideas, norms and beliefs expressed or reflected in symbols, rituals, myths and practices that shape how an organization functions and adapts to external stimuli and that give meaning to its members'*.[4]

However – and of particular note here –the authors discuss the military culture of each component (Army, Navy, Marines or Air Force) within the military of one particular nation (the USA, Great Britain, Japan etc.). For a military organization made up of components drawn from 29 nations, instead of discussing military culture, it may be more useful to consider cultural interoperability. Winslow and Everts (2001)[5] do exactly that in their analysis of the IFOR mission in the former Yugoslavia in the late 1990s:

'However, in our opinion, it is not only system interoperability but operational and particularly cultural interoperability – the shared way by which NATO armies "do business" – which is a factor contributing to mission success.'

So what stops us doing MDO now? At its most basic, it is a human problem and one that arises out of our willingness to let technology solve

problems for us. And yet cultural interoperability is part of the NATO DNA – and this strength was observed (by Winslow and Everts, for example) as long ago as 2001 and (had it been looked for) probably for much longer. Far from being intractable, NATO staffs and command structures tackle the 'monkey first' problem every day. One of the ways that they do this is by working together as a team.

NATO's strengths lie in the very diversity of its members and, whilst 'cultural factors' may continue to infuriate and exasperate us, they may also form one of NATO's critical capabilities. At the very least, they form a toolset for handling complexity, and breakthroughs happen when we get into these uncomfortable spaces.

One recommendation that resulted from this discussion of culture and / or cultural interoperability is that NATO – perhaps through the agency of the JAPCC – may want to examine and define its existing culture (more likely 'cultures') in the 21st Century before it can set about trying to adapt or change it / them. It is difficult to get to a known destination if you're not sure of your actual starting point. The JAPCC is ideally placed to do this – it is small enough for observations to be made easily and it contains a robust (if non-homogeneous) mix of nationalities

THEME 4: Trusted Autonomy

The use of the term 'cyber' rather than 'cyberspace' was rightly cautioned against. The word 'cyber' is sometimes used as an all-encompassing term to include cyberspace, cyber-attacks, cyberwar etc. However, we risk being imprecise by using the adjectival prefix 'cyber' without a suffix. This comes back to General Townsend's entreaty to strive to use the right words in the right context. This is something that is even more important to an alliance where everyone (native speakers included) may not have a complete encyclopaedic command of the common language.

Cyberspace is sometimes seen as a place inhabited and only fully understood by 'bright young techno-geeks' – a term that could be used to describe only a minority of conference delegates. There is a need for all decision-makers to educate themselves about this often misunderstood domain. Just as senior leaders grasped the nettle of learning more about space, so they must also do when it comes to cyberspace. A concept that can often be useful in determining the acceptability of computer-based technologies is that of 'digital natives versus digital immigrants'. This comes back to the word 'young' in the earlier phrase 'bright young techno-geeks'.

In their lifetimes, digital natives never knew a time when things like email, social media and the internet did not exist. The rest of us – the digital immigrants – still remember sending memos and reading about things that happened yesterday from quaint sheets of paper that made our hands dirty.

It is, perhaps, easy to jump to the conclusion that digital natives will be more accepting of technology making decisions on behalf of humans; that digital natives believe what the machine says, without questioning the decisions made – by AI – on our behalf. However, as one memorable exchange at the conference showed, our young people are well educated and more than happy to question not just the decisions made by machines but also the assumptions of their elders. This presents its own unique opportunity, whereby NATO leadership and staff (led by the NAC), being comprised of necessarily senior leadership, will be challenged to adapt to new technologies and leverage younger expertise. This theme of 'trusted autonomy' is explored in more detail later in this paper.

Discussions as a result of questions from the floor are often fertile ground for new ideas. One such discussion was based on the premise that, the 'plethora of effects available to NATO' demands that we get the C2 correct. Multi-domain C2 suitable to meet the demands of MDO can be likened to the OODA loop of a person riding a bike. Countless continuous inputs are being made with constant feedback far faster than human consciousness would allow. This is clearly more complex than deciding on which effect

for which target, but it does illustrate the C2 dilemma in deciding (for example) whether to use an effect in the cyberspace domain to jam the lifting system of a bridge as opposed to bombing it. Whilst the first effect may enable NATO forces to use the unscathed bridge themselves to facilitate manoeuvre, the Battle Damage Assessment (BDA) dilemma is made much easier if the kinetic effect is chosen – it's easier to identify a destroyed bridge than it is to identify a bridge that can't be opened or closed because of some invisible disruption to its electronic control system.

As airmen, we must learn to move beyond the traditional ways of thinking which rely solely on kinetic force to degrade capabilities as the 'old way of doing things'. Mastery of the cyberspace domain will enable NATO to be smarter and to use 'new' ways of doing things.

Exercises and wargames are the ideal places to test out such dilemmas and to learn lessons for these new ways of operating. However, as later conference panels observed, whilst training is mostly what NATO does, it is not always as realistic as it could be. MDO tailored training – both live and synthetic – is needed so that NATO can truly make the transition from lessons observed to lessons learned. Very cost-effective and realistic synthetic training has become a reality– through advances in AI and augmented reality (AR) supported by so-called 'Big Data'. Big data has been characterized as the art of finding one particular snowflake in a blizzard. Again, the JAPCC is already taking a leading role in synthetic training. As this is being written, a team of JAPCC SMEs is providing OPFOR for Exercise TRIDENT JUPITER at Joint Warfare Centre (JWC) Stavanger.

Human-on-the-Loop versus Human-in-the-Loop

One of the key takeaways from the earlier theme of human factors and military culture was that humans will often differ in their willingness to allow technology to help them solve problems – particularly when, to do so, they must allow machines to have some level of autonomy. Sometimes,

a lack of willingness to do this stems from a belief that autonomy is a case of 'all or nothing' – when, in actual fact, there exist clearly defined levels of autonomy and our daily lives already depend on them.

A 2016 article in Resilience Week by Nothwang et. al.[6] is one of the early published uses of this phrase (in a military context) which also gives useful definitions and examples. The paper 'investigates the contributors to success/failure in current human-autonomy integration frameworks, and proposes guidelines for safe and resilient use of humans and autonomy with regard to performance, consequence, and the stability of human-machine switching'. It classifies four levels of autonomy, and defines them, from lowest autonomy to highest autonomy, as:

- Human – where 'the human is actively involved in all aspects of an agent's task'.
- Human-in-the-loop (HITL). This is where humans 'actively (often continuously) engage in control decisions'.
- Human-on-the-loop (HOTL). This implies 'supervisory control where the human monitors the operation of autonomy, taking over control only when the autonomy encounters unexpected events or when failure occurs'.

- Complete autonomy (CA) where 'the human has a minimal task load for decision-making, is not the ultimate arbiter on decisions, and is only minimally involved in agent decision-making'.

These definitions are of use to us, not least in furthering our understanding of when the HITL / HOTL terms are being used incorrectly.

Nahavandi's 2017 paper – 'Trusted Autonomy between Humans and Robots' takes our understanding one stage further when it states that:

'Machines that carry out a task for a time period, then stop and wait for human commands before continuing are known as "HITL systems", while machines that can execute a task completely but have a human in a monitoring or supervisory role, with the ability to interfere if the machine fails, are known as HOTL systems.' [7]

This is not science fiction. These machines are well known to us. That annoying disclaimer that pops up every time we try to use our in-car satnav (and demands that we press our grubby fingers on a screen icon before it will deign to continue) is a crude example of a HITL system. Commercial airline pilots can rely on their aircraft to auto land at suitably equipped airports, but they remain in their seats alert and ready (we hope) to intervene if something out of the ordinary happens. This is a HOTL system. HOTL technology with military applications is becoming increasingly relevant with the advent of autonomous wingmen and swarming concepts.

It is, perhaps, the concept of CA – complete autonomy – that scares us and brings to mind the 'killer robots' scenario so beloved of the movies. Robotics and autonomous systems (RAS) are the emergent technologies of the 21st Century and, as yet, may not be widely understood. RAS is enabled by artificial intelligence and machine learning and these are things that concern some of the great minds of our time. The recently deceased cosmologist, Professor Stephen Hawking sounded this note of caution as recently as 2014:

'The development of full artificial intelligence could spell the end of the human race … It would take off on its own, and re-design itself at an ever-increasing rate. Humans, who are limited by slow biological evolution, couldn't compete and would be superseded.'[8]

Whilst we should heed Professor Hawking's warning, we should not let it prevent us from harnessing AI and machine learning to help NATO to ensure the collective defence and security of our Alliance.

Conclusion

'For NATO, every day of peace is a victory.'

Conferences tend to come and go. The initial enthusiasm for what has been discussed and what has been decided can sometimes be forgotten in the pressure to get back to the 'day job' and to contend with all the problems that have been waiting back in the office. However, the JAPCC now has a responsibility to ensure that the key takeaways from this conference are, firstly, not forgotten but, much more importantly, to ensure that concrete actions are taken to advance the discussion and implementation of MDO for NATO.

So how can the JAPCC play a part in moving the Alliance forward? It was stated during the conference that MDO requires three things: Connecting, Decision-Making, and Responding at Speed. To do this, NATO requires a networked force with resilient and self-healing mesh networks. NATO cannot afford to wait until it has the perfect set-up for this or until the perfect solution is in place. It needs to take incremental steps towards this every day. The NATO alliance, assisted by its centres of excellence, is an ideal environment in which to 'Connect, Share and Learn'. One example of this was ably demonstrated by representatives from the C2COE at the conference

in their presentation on the tools required to support MDO. As they said, 'The Dodos did not go extinct because of the Dutch who ate them … but because they were simply not multi-domain'.

It was sobering to learn – in the example about GPS jamming from Russian ships in the Eastern Mediterranean – that one of NATO's potential adversaries may be embracing the principles of mission command that we long believed were much more likely to be used by NATO. Procedures supported by a mix of legacy technologies and lengthy chains of command – where decisions must be relayed upwards for ultimate approval to then come back to commanders in the field – are not the way to conduct operations in the 21st Century. If they are, then we can be sure that more agile opponents will be aware of this and use it to their advantage.

Resilience is a term that is often used to describe the electronic networks needed to support processes. However, resilience is also needed in the human networks – the command structures from operational level and on to tactical levels – when far-reaching decisions need to be taken rapidly. Some evidence suggests that C2 paradigms may have reversed between East and West since the early 1990s. The Iraqi IADS and military in 1991 were defeated because they were slow, centrally controlled and relied on things like Ground-controlled Intercepts and excessively centralized control that killed initiative, while the coalition was much more decentralized and flexible, and our OODA loop was therefore much tighter. With many engagement authorities being delegated down to Russian ship captains in the Black Sea, for example, while NATO forces have to wait for 29-nation NAC approvals, it seems the situation may have reversed and is no longer in the Alliance's favour.

Despite the fact that state-of-the-art technologies already exist to support military decision-making processes, NATO Joint Headquarters continue to utilize office software packages (e.g. MS PowerPoint) as one of their visualization tools to support decision-making. Inefficiencies in C2 processes rapidly become a critical vulnerability for a military organization that needs

to respond to multiple threats at speed. The two CoEs – the JAPCC and the C2COE – should work together to develop, test and evaluate tools that can be used to enable enhanced situational understanding at the operational level and embed efficient and effective processes that can be executed rapidly and with fewer people having to give their approval. Dedicated tools are required to enable synchronization and deconfliction – and going forward these tools must incorporate interoperability by design, and not wait to address it post-production.

The JAPCC – with its proven expertise and regular involvement in supporting NATO Joint Exercises – is ideally positioned to work with colleagues from other CoEs and other NATO organizations to take this forward and it will form one of the strands of the JAPCC's programme of work for 2020/21.

It is easy to be a pessimist and to believe that MDO is either some sort of illusory nirvana or that, if real, MDO is all too difficult to achieve. What the 2019 JAPCC Conference helped to demonstrate is that, in actual fact, MDO is neither of these two things.

One result of the conference has been a draft definition of what is meant by the term MDO. This gives NATO a starting point to begin building doctrine for MDO. Projects such as the federated mission network (FMN, discussed earlier), show NATO's resolve to fully understand and protect cyberspace. The US has made (and continues to make) great strides in protecting space and ensuring NATO's unfettered access to the key capabilities derived from space. The smaller nations are also beginning to play their part here.

However, there is much work still to be done and the JAPCC stands ready to play its part in doing it. The MDO narrative continues in the C2COE seminar on the subject, to be held in Bratislava in June of 2020. MDO is not going to go away and the 2020 JAPCC Conference will develop the theme further when it takes as its aim …

Leveraging Emerging Technologies
in Support of NATO Air & Space Power

See you there!

References

1. Air Force Magazine (2019) Shriever Wargame Drives Command and Control Change at CSpOC. [online]. Available from http://airforcemag.com/Features/Pages/2019/September%202019/Schriever-Wargame-Drives-Command-and-Control-Change-at-CSpOC.aspx [Accessed 2 Nov. 2019].
2. Bower, M. 1966. The will to manage. New York: McGraw-Hill.
3. Handy, C. 1976. Understanding Organizations. London: Penguin.
4. The Culture of Military Organizations. 2019. Edited by Mansoor and Murray: Cambridge University Press.
5. Winslow D., Everts P. (2001) It's Not Just a Question of Muscle: Cultural Interoperability for NATO. In: Schmidt G. (eds) A History of NATO – The First Fifty Years. Palgrave Macmillan, London.
6. Nothwang W. D., McCourt M. J., Robinson R. M., Burden S. A. and Curtis J. W. (2016) The human should be part of the control loop? Resilience Week (RWS), Chicago, IL, 2016, p. 214–220.
7. Nahavandi S. (2017) Trusted Autonomy Between Humans and Robots. IEEE Systems, Man and Cybernetics Magazine, 17 Jan., p. 10–17.
8. BBC (2014) Stephen Hawking warns artificial intelligence could end mankind. [online]. London: BBC, Available from https://www.bbc.co.uk/news/technology-30290540 [Accessed 29 Oct. 2019].

JAPCC invites you to attend the

2020 | AIR AND SPACE POWER CONFERENCE

Leveraging Emerging Technologies in Support of NATO Air & Space Power

6–8 October 2020, Essen, Germany

Joint Air Power Competence Centre

www.japcc.org/conference

Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140 | 47546 Kalkar (Germany) | www.japcc.org

Follow us on Social Media: