Joint Air & Space Power Conference 2021

Delivering NATO Air & Space Power at the Speed of Relevance

7–9 September 2021

READAHEAD

Joint Air Power
Competence Centre

Delivering **NATO Air & Space Power** at the **Speed of Relevance**

DELIVERING NATO AIR AND SPACE POWER AT THE SPEED OF RELEVANCE
JAPCC JOINT AIR AND SPACE POWER CONFERENCE 2021

*READ***AHEAD**

Delivering
NATO Air & Space Power
at the **Speed of Relevance**

Joint Air and Space Power Conference 2021

Acknowledgements
This read ahead is a JAPCC product realized in collaboration with the authors of the essays contained herein. The JAPCC would like to thank the numerous authors who took the time to contribute to this product in an effort to advance this topic for discussion within NATO.

Editorial Team
Brig Gen Sgamba
Col Brad Bredenkamp
Col Matthew Willis
Lt Col Henry Heren
Maj Osman Aksu
Maj Massimo Di Milia
Maj Andreas Wurster
Mr Simon J. Ingram
Sgt1 Lilian Brandon
Mr Sascha Kranefeld
SSgt Marcel Jammoul
Ms Britta Klein

Disclaimer
The views expressed in this work are those of the authors. It does not represent the opinions or policies of the North Atlantic Treaty Organization (NATO), and is designed to provide an independent overview, analysis and food for thought regarding possible ways ahead on this subject.

Published and distributed by
The Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140
47546 Kalkar
Germany

M Denotes images digitally manipulated

Moderator's Foreword

Esteemed Colleagues,

I am extremely excited about the prospect of participating in the JAPCC's Joint Air & Space Power Conference this year. Much can be achieved, as we have all learnt, through online 'virtual' meetings, but we have also experienced their limitations when compared to meeting 'in real life'. I am currently imagining being in a large room with actual people, listening, meeting and chatting together, face-to-face, and then over coffee during the breaks. I wonder if any of us will remember how this 'normal' human interaction actually happens and how well we will adjust back to something we once took for granted?

As I write this on a dull early March morning in England, there are still four more weeks until I can visit the hairdressers and (legally) get a proper haircut – so at least another four weeks of getting a shock every time I look in a mirror. On the more positive side, I have just had my first vaccination shot and this seems to present the way out of this threat to all of us. But, whilst lockdown rules and regulations may have been different for all of us depending on our locations and personal circumstances, the challenges we face are more uniform – and they have continued to evolve. I do not just mean the challenges presented by the global pandemic, but also those presented by the changing world order.

The security challenges to NATO did not just get put 'on hold' as our individual countries turned inward to battle the existential threat to survival at home. Indeed, the global pandemic also presented an opportunity to NATO's near-peer adversaries to manoeuvre and attempt to gain an advantage. How successful they may have been in doing this is, perhaps, yet to be determined, but we can be sure that any return to 'business as usual' for global defence and security will forever retain a watermark of the COVID-19 crisis – and be indelibly marked and changed by it.

The theme of the conference this year is 'Delivering NATO Air and Space Power at the Speed of Relevance', but what does this actually mean? In recent years, the term 'speed of relevance' appeared in several defence-related high-level papers. The 2018 US National Defense Strategy links the term to the need to reform processes in the US Department of Defense to facilitate quicker decision-making on the modernization of the armed forces. The term made its way subsequently in many NATO and NATO-related documents where it was used with respect to ensuring readiness, providing options to the Alliance as well as agile, flexible and effective Command and Control in support of NATO's core tasks.

From my preliminary reading (outlined above) about this term, it is clear that – unlike the speed of light – the speed of relevance is a dependent variable. But what does it depend on and what are the metrics that can be used to measure 'relevance'? This is something that I hope the five panels will explore in their discussions and I urge conference delegates to consider these points as well. The conference panels will explore how five key areas relate to the conference theme:

- Policy and Strategy
- Dynamic C2 Synchronized Across Domains
- Superiority in the Electromagnetic Spectrum
- NATO Space

The consultation process for the development of NATO's Political Guidance 2023 which will provide decisive guidance for capability planning is supposed to start soon after our September conference. It is, therefore, extremely timely that the conference takes place when it does and that the JAPCC has managed to gather so many senior decision-makers and deep thinkers together in one place – from NATO and beyond. This conference represents a unique opportunity for us to spend a significant amount of time together, discussing and determining the challenges that we all face. In terms of conference outcomes, there is no reason why we should not aim high. However, we should also bear in mind that we will arrive in Essen in early September with a big bag of extremely complex questions. Even with all the firepower that the conference can muster, we will not, realistically, come away with the same big bag filled with all the answers to those same complex questions. What we can expect, and what we can all work towards will be a better understanding and, perhaps, a reframing of how we might react and adjust our thinking and our ways of doing business.

The JAPCC has worked tirelessly to get this conference back on track after the hiatus of the last year and a half. This year, once again, they have put together a carefully curated selection of articles which set the scene for each of the panels. If we are to take the most value from (and make the greatest contribution to) the panel discussions, we will need to read these articles in advance. In the days and weeks after the conference, I know that the JAPCC will continue to work tirelessly to construct a summary of what was discussed – and then use that summary to draw concrete conclusions to share with us all. I am delighted and proud to have been asked back this year to assist, in my own way, with these tasks. I look forward to meeting you all in September.

Bruce Hargrave BSc MBA
Independent Air and Space Power Advisor

Table of Contents

Table of Contents

Table of Contents

Table of Contents

[M] © garagestock/Shutterstock.com

Policy and Strategy – Panel Introduction

1

From the Washington Pact to NATO 2030

By Maj Massimo Di Milia, IT Air Force
Joint Air Power Competence Centre

Introduction

As the Alliance seeks to build resilience both within the individual nations and across the command structure, synchronizing the focus and efforts for collective defence requires open dialogue and consensus on how to proceed together. The ability of the Alliance to harmonize its efforts and minimize force capability deficiencies is vital. This ability includes exploring opportunities for joint education and training across disciplines and operational domains. It also necessitates the ability to integrate emerging technologies with existing capabilities, as well as anticipate the integration of future developments, to ensure maximum exploitation of the dynamic relationships across the force structure. The Alliance must also seek to stress the importance of information sharing, to include education across operational domains and inclusion into doctrine and strategy ways in which to adapt and merge new capabilities into current operations as they become available. Finally, the Alliance needs to harmonize policies, both of NATO and its member nations, to establish a common approach which will enable faster consensus-building and decision-making in times of crisis.

The Evolution of Strategic Concept

For the purposes of this paper, since the inception of NATO, there have been three periods during which NATO's essential reasoning and strategic thinking has evolved:

- the Cold War;
- the immediate post-Cold War;
- the security environment since 9/11.

The Alliance's first strategic concept stated that the primary function of NATO was to deter aggression and that NATO forces would only be engaged if this primary function failed, and an attack was launched. Complementarity capabilities between members and standardization across the Alliance were also key elements of this concept. Each member's contribution to defence should be in proportion to its capacity – economic, industrial, geographical, military – and cooperative measures were put into place by NATO to ensure the optimal use of resources. Numerical inferiority in terms of military resources, vis-à-vis the Soviet Union was emphasiszed. After 1991, a more extensive methodology was embraced where the ideas of participation and security supplemented the essential ideas of deterrence and defence.

From 1949 until the end of the Cold War, NATO published three Strategic Concepts, joined by new doctrine that distributed the measures by which the military was to actualise the Strategic Concept, entitled Strategic Guidance,[1] 'The Most Effective Pattern of NATO Military Strength for the Next Few Years',[2] and 'Measures to Implement the Strategic Concept'.[3]

It can also be said that from 1949 to 1991, NATO's strategy was largely characterized by defence and deterrence, although with growing attention to dialogue and détente for the last two decades of this period. International relations were dominated by bipolar confrontation and the focus was more on tension, than it was on dialogue and cooperation. In the post-Cold War time frame, a broader approach was adopted where the notions of cooperation and security complemented the basic concepts of deterrence and defence. For the Alliance, the period was characterized by dialogue and cooperation, as well as other new ways of contributing to peace and stability, such as multinational crisis management operations.

During this period, the three unclassified Strategic Concepts released by NATO were supplemented by characteristically military documents (MC Directive for Military Implementation of the Alliance's Strategic Concept,[4] MC Guidance for the Military Implementation of the Alliance Strategy,[5] and MC Guidance for the Military Implementation of NATO's Strategic Concept),[6] which reflected the change of thinking and priorities for the Allies. These non-confrontational documents were released to the public. While maintaining the security of its members was their fundamental purpose (i. e., collective defence), they sought to improve and expand security for Europe through partnership and cooperation with former adversaries. They also reflected a desire to reduce the number of nuclear forces to a minimum level, that which was only sufficient to preserve peace and stability. These documents stated that the Alliance's fundamental tasks were security, consultation, and deterrence and defence, adding that crisis management and partnership were also essential to enhancing security and stability in the Euro-Atlantic area.

In 1999, shortly after NATO's 50-year commemoration, Allied leaders adopted a new Strategic Concept that committed members to common defence, peace, and stability of the more extensive Euro-Atlantic zone. It depended on a broad definition of security which recognized the importance of political, economic, social, and environmental factors in addition to the defence dimensions. It recognized the new dangers that had arisen since the end of the Cold War, which included: terrorism, ethnic conflict, human rights abuses, political instability, economic fragility, and the proliferation of nuclear, biological, and chemical weapons and their means of delivery.

The 9/11 terrorist attacks against the United States brought the danger of psychological warfare and weapons of mass destruction to the forefront. NATO needed to protect its populations both at home and abroad. Accordingly, NATO went through major internal changes to adjust military construction plans and training capacities to prepare individuals for new assignments.

Since the terrorist attacks of 9/11, NATO's military thinking, assets, and energy have concentrated on the battle against terrorism and the prevention of the spread of weapons of mass destruction. NATO has deployed troops beyond the Euro-Atlantic zone and grown to include 30 member nations. However, new dangers have arisen like energy security and cyber-attacks. These were among the components that prompted Alliance experts to deliver another Strategic Concept in 2010.

NATO continues to develop and broaden its partnerships and quicken its pace of change to build new political connections and develop more solid operational capabilities to face an undeniably changing and more unstable world order.

With all this history in the back of our minds, it is necessary to proceed a step further with the biggest priority for NATO being to remain strong militarily and to become even stronger politically to take a more global approach. In November 2020, NATO leaders released an updated strategic concept entitled NATO 2030.

NATO 2030 is bringing together Allied parliamentarians, civil society, public and private sector experts, and youth to provide fresh thinking on how to make NATO an even stronger Alliance.

Additional Articles

This section presents five articles which will introduce various ideas and issues intended to inform the Harmonised Policy & Strategy Panel discussion, the ideas expressed in these articles are meant to inspire critical thinking and to prepare those attending the 2021 Joint Air & Space Power Conference:

- In ***Increasing NATO's Resilience***, Mr Omree Wechsler and Mr Doron Feldman address the problem of disinformation campaigns launched within NATO states,[7] with the aim of undermining public support within the Alliance and provoking division among its member states. In their paper, the authors suggest a soft power approach to preserve the Alliance legitimacy and cohesion and to promote further cooperation with member and non-member states.[8]

- The next paper, ***Looking for a Few Good Operators***, by Dr Kyleanne Hunter, addresses the issue of Opportunities for Space Force to fulfil NATO's Women, Peace, and Security Agenda.[9] The unique nature of the Space domain, touching and enabling operations in every other domain, provides an opportunity to meaningfully enact gendered perspectives across all operations.

- ***The Impact of Law on NATO's Space Power at the Speed of Relevance*** appears next in the book. Mr Álvaro Blanco, Col Dan Gallton, and Mr Dale Reding begin treating the interplay between concepts and constraints associated with the development of an overarching Space policy. The focus is on the extent of the collective self-defence umbrella towards the Outer Space domain and concludes with several significant international legal concepts that will impact future NATO Space operations.

- Ms Gentry Lane's ***Avoiding Cyber Forever Wars*** focuses on how to disallow further adversary advancement in the Cyberspace domain and how essential it is for NATO partners to accelerate agreement on desired ends, cohesive strategies, and a quantifiable framework for assessing the progress of ways and means established to deter adversary cyber aggression. She advises that the force with the most effective use of cyber weapons, tactics, techniques, and procedures to achieve the desired ends, will be the victor, not intended as a Clausewitzian ideals of defeat or surrender, but in achieving strategic objectives.

- The final paper for this panel represents food for thought for novel Space security diplomacy. In ***Outer Space, a Challenging Domain for Ambitious Defence Strategy***, Dr Anne-Sophie Martin explains how a variety of actors subsist in the most recently recognized operational domain[10] and how they can be 'intimidating' by conducting acts of espionage or carrying out anti-satellite tests. This leads to the use of satellites in order to conduct military operations as Space systems have become strategic targets that can be hacked or jammed to weaken an adversary.

Major Massimo Di Milia (IT AF) is currently stationed at the JAPCC, Kalkar, as Air Transport expert in the Air Operation Support Branch. He is a C130J pilot with almost 20 years' active-duty service. His career has sent him flying all over the globe, executing missions of airdrop, air-to-air refuelling, and assault operations.

Endnotes

1. Dr Pedlow, G. W., 'NATO Strategy Documents 1949–1969' (1997), available at: https://www.nato.int/docu/stratdoc/sd49-69e.htm (accessed 12 Feb. 2021).
2. NATO Military Committee, North Atlantic Military Committee Decision on M.C. 48, The Most Effective Pattern of NATO Military Strength for the Next Few Years, 22 Nov.1954, p. 229, available at: https://fransamaltingvongeusau.com/documents/dl2/h3/2.3.4.pdf (accessed on 31 Jan. 2021).
3. NATO Military Committee, Final Decision on MC 48/3, Measures to Implement the Strategic Concept for the Defence of the NATO Area, 8 Dec. 1969, p. 371, available at: https://www.nato.int/docu/stratdoc/eng/a691208a.pdf (accessed on 31 Jan. 2021).
4. North Atlantic Treaty Organization, 'Strategic Concept' (2020), available at: https://www.nato.int/cps/en/natolive/topics_56626.htm (accessed 20 Feb. 2021).
5. Dr Pedlow, G. W., 'NATO Strategy Documents 1949–1969' (1997), available at: https://www.nato.int/docu/stratdoc/sd49-69e.htm (accessed 15 Mar. 2021).
6. Spily, P., Necas, P., 'Alliance's Strategic Concept' (2009), 4 (2) 95-100, available at: https://search.proquest.com/openview/fd3c5a60982bd499d69d1f037e6c7e25/1?pq-origsite=gscholar&cbl=54467 (accessed 28 Feb. 2021).
7. Dizikes, P., 'Study: On Twitter, false news travels faster than true stories', MIT News, https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308, 8 Mar. 2018 (accessed 15 Jan. 2021).
8. NATO, Brussels Summit Declaration: 'Issued by the Heads of State and Government participation in the meeting of the North Atlantic Council in Brussels 11–12 Jul. 2018', available at: https://www.nato.int/cps/en /natohq/official_texts-156624.htm (accessed 13 Jan. 2021).
9. NATO, 'Women, Peace and Security', last updated 1 Oct. 2020, available at: https://www.nato.int/cps/en/natohq/topics_91091.htm (accessed 12 Feb. 2021).
10. Blount, P. J., 'Space Security Law', Oxford Research Encyclopedias, 25 Jun. 2018.

M © Pan Andrii/Shutterstock.com

The Impact of Law on NATO's Space Power at the Speed of Relevance

11

By Mr Álvaro Martín Blanco,
Col Dr Daniel Gallton, US Air Force, and
Mr Dale Reding
NATO Science and Technology Organization/NATO HQ

Introduction

The Space security landscape has become increasingly complex and critical to operational success. Allied leaders have recognized Space as a highly dynamic and strategically relevant environment – critical to the Alliance's core tasks of collective defence, crisis management, and cooperative security. In 2018 this led to NATO leaders agreeing to the development of an overarching Space policy.[1] In 2019, as part of this development, NATO officially recognized Space as an operational domain on par with and linked to the Land, Maritime, Air, and Cyberspace domains. In parallel NATO leaders have identified Space technologies as one of seven critical emerging and disruptive technologies essential for the Alliance to maintain a technological edge.

The NATO Science and Technology (S&T) Organization (STO) has responded to these developments by undertaking a comprehensive review of its Space S&T activities and developing a multi-year strategy for Space S&T development. For this review, a series of intense workshops were conducted by the Systems Concepts and Integration (SCI) panel. These workshops explored several potential areas for Alliance S&T collaboration and identified significant factors (concepts and constraints) associated with such development. This paper treats the interplay between two of these identified factors, the need to respond at the 'speed of relevance' and the practical implications of an ambiguous Alliance Space legal framework.

The Speed of Relevance is a modern concept with multidimensional reach and applicability. It reflects the evolving organizational culture of defence organizations and the need for more efficient and effective decision-making processes, within increasingly complex strategic environments.[2] In order to deliver Space-derived Data, Products, and Services (DPS) at the Speed of Relevance, the NATO Alliance (Alliance) must ensure that it complies with the international legal framework established under the North Atlantic Treaty (Treaty), the 'pierre angulaire' of the Alliance, which is in line with overarching regulations by the United Nations.

Article 3 of the Treaty states that the NATO Allies (Allies) must act together, continuously and effectively to achieve Allied objectives.[3] With this in mind, the Alliance currently does not plan for the foreseeable future to procure NATO-owned Space systems, but instead, is planning to continue relying on Ally-owned assets. This decentralized Space capability requires an enhanced degree of cooperation and coordination among Allies regarding Space DPS, interoperability and evolving Space legal frameworks and policies.

Consequently, the authors examine current international legal frameworks regarding Space law and the role of harmonization to foster legal and policy interoperability. We then focus on the extent of the collective self-defence umbrella towards the Space domain and conclude with several significant Space international legal concepts that impact future NATO Space operations.

Domestic Space Legal Frameworks and NATO: Regulatory Competition vs Harmonization

Outer Space is becoming increasingly accessible to new actors due to increased affordability, technology proliferation, and commercial sector innovation. Consequently, Space activity is expanding globally, and many Allies are developing domestic Space legal frameworks to attract investment capital, increase Space commerce, and compete globally. Simultaneously, the increasingly congested, contested, commercial, and competitive nature of Space operations intensifies the need for legal clarity and harmonization. These legal frameworks attempt to regulate the Space sector and fill the gaps where international Space law is open for interpretation. However, there is a lack of consistency between such national frameworks, with some nations having comprehensive overarching policies beyond the basic instruments of international Space law and others not having ratified the basic instruments of international Space law.

At the same time, the development of multiple domestic legal frameworks across different Allied jurisdictions may result in regulatory competition. Unless checked, such competition inevitably leads to the progressive dismantling of regulatory standards or a 'race to the bottom'. This phenomenon occurs 'under conditions of economic interdependency between jurisdictions, when one state lowers its regulatory standards in order to attract investments'.[4] A race to the bottom could ultimately damage the interoperability of the Space legal frameworks of the Allies. In the end, this diminishes the collective value of NATO Allies' Space assets and negatively impacts NATO Space power projection.

To avoid regulatory competition and a lack of coordination among frameworks and policies, the NATO Alliance is in a position to use its prominence and influence to promote a dialogue favouring the harmonization of national Space legal frameworks. The harmonization process should not create a single or unique legal framework for the Alliance. Instead, it should focus on fostering a common legal Space doctrine based on agreements regarding fundamental mechanisms, international standards, or norms of behaviour.

Space interoperability is enhanced if the NATO Alliance builds a framework in which its Allies can collaborate using operational assets and respective national policies or frameworks. Therefore, a harmonious legal collaboration could enable decision-makers to make synchronized decisions in a complex decentralized environment more rapidly, or, if you prefer, at the Speed of Relevance.

To accomplish this goal, the NATO Alliance needs to define the North Atlantic Treaty's applicability in the Outer Space domain using this as the developmental foundation of a comprehensive Space legal architecture. The authors highlight several critical issues in extending the Treaty to the Space domain in the following section.

The North Atlantic Treaty and the Outer Space Domain

In 2019, the NATO Alliance recognized Space as an operational domain; however, the North Atlantic Treaty (Treaty), which is the foundation of the NATO Alliance, was signed in 1949 and hence does not acknowledge Outer Space within its articles. While the Treaty does not deny parties the possibility to carry out operations in Outer Space, the Treaty's wording makes it unclear whether NATO's collective self-defence' umbrella, provided through Article 5, would apply to the Space operational domain.

The wording of Article 6 of the Treaty, which defines an armed attack for Article 5, states that an armed attack is as an attack:

- 'on the territory of any of the Parties in Europe or North America, on the Algerian Departments of France, on the territory of Turkey or on the Islands under the jurisdiction of any of the Parties in the North Atlantic area north of the Tropic of Cancer;
- on the forces, vessels, or aircraft of any of the Parties, when in or over these territories or any other area in Europe in which occupation forces of any of the Parties were stationed on the date when the Treaty entered into force or the Mediterranean Sea or the North Atlantic area north of the Tropic of Cancer'.[5]

According to the Outer Space Treaty (OST)[6], Outer Space is not subject to national appropriation by claiming sovereignty or any other means available to a nation-state. Thus, if Allies are unable to extend national sovereignty to Outer Space there are some questions that can be asked:

- Could an 'armed attack', as defined in article 6 of the Treaty, ever occur in Outer Space?
- If so; would the concept of an 'armed attack', as defined in article 6 of the Treaty, apply to the forces, vessels, or aircraft of the Allies while in Outer Space?
- Should armed attacks on commercial satellites, installations, or networks fall inside the Treaty's terms?

The lack of clarity of this provision of the Treaty weakens the Alliance's options for deterrence. Indeed, it may threaten the rapid delivery of Space Power at the speed of relevance. Nevertheless, NATO has options to address this situation. The authors believe that the Alliance should:

- Build on previous cyber-attack declarations[7] to issue a formal declaration stating the readiness to counter attacks on Allied Space assets, Including an explanation of which assets fall within the scope of the Treaty.

- Consider adopting Treaty instruments that would include attacks against Space assets.

The Clarification of Significant Space International Legal Concepts

The international legal framework that governs Space activities contains several areas open for interpretation. Perhaps the most critical are:

- **The boundary between airspace and Outer Space:** When we refer to Outer Space as an operational domain, it seems apparent that we are referring to a domain different from the operational air domain; but legally speaking there is no clear border between these two. International law has yet to define the frontier between airspace and Outer Space unambiguously.[8]

  The importance of defining this boundary relies on the fact that international Space law is different from international air law, impacting air operations. NATO decision-makers have an opportunity to explicitly define the operational border between these two domains for the Allies, bearing upon Space operations.
- **Peaceful use of Space:** The preamble of the OST[9] recognizes Outer Space for peaceful purposes, but it does not define the term. However, it establishes a particular legal regime on celestial bodies, declaring them a demilitarized zone, and bans the stationing of weapons of mass destruction in Outer Space.

  This lack of definition and precision on the language has originated two approaches among the OST signatory nations. On one side, several countries have adopted the position that peaceful means 'not aggressive'; on the other side, several member nations have adopted a position that peaceful means 'non-military'.[10]

  There is a clear limit regarding the use of force, irrespective of the chosen definition of peaceful purposes in the OST text. Article 2 (4) of the

UN Charter[11], provides such a limit applicable to Outer Space along with the exceptions stipulated in the UN Charter and general international law through article III of the OST that applies the principles of international law to the territory of Outer Space.

To address Alliance interoperability challenges, the Allies have to agree on the definition of numerous imprecise international legal terms. The authors believe that NATO is an ideal platform for raising awareness of this issue and developing such an agreed Space legal international framework while harmonizing differing criteria across its Allies. This is true whether NATO acts directly or as a catalyst for such a discussion.

Conclusion

To move forward in the operationalization of Space, the NATO Alliance requires an agreed regulatory and legal environment. The lack of clarity of the North Atlantic Treaty and the legal vacuum regarding the international legal framework are stumbling blocks that 'could provide one iota of decision advantage to potential adversaries at a great cost'.[12]

The SCI workshop noted that to deliver Space power at the speed of relevance, the NATO Alliance should:

- Encourage the development of the operational and legal frameworks through which the Allies can collaborate via both operational assets and their respective national policies and frameworks.
- Clarify the applicability of the North Atlantic Treaty to Outer Space and use the Treaty as a foundation towards achieving the first objective; Work towards the establishment of a forum to synchronize international legal concepts across the Allies.

NATO has a unique opportunity to become an international leader in synchronizing Space legal frameworks and policies. At the same time, it can promote dialogue between the Allies and build upon their Space Policy. These are small but critical first steps to ensure reliable access to Space services and harmonize the Alliance's approach to Space security.

Mr Álvaro Martín Blanco is part of the Operations and Coordination Division in the North Atlantic Treaty Organization (NATO) Science and Technology Organization (STO) Collaboration Support Office (CSO), Paris, France. He graduated from the University of Zaragoza in 2018 with a Bachelor's degree in Law. He completed an LL.M in Legal Practice at the University of Zaragoza in March 2020 and obtained the Spanish Lawyer's Professional Title (Título Profesional de Abogado) in July of 2020.

Colonel Daniel A. Gallton (US Air Force) is the Head of the Operations and Coordination Division in the North Atlantic Treaty Organization (NATO) Science and Technology Organization (STO) Collaboration Support Office (CSO), Paris, France. Colonel Gallton graduated from the Pennsylvania State University in 1994 with a BS in physics. He completed an MS in Physics in 1998, an MS in Strategic Security Studies in 2012 at the Naval Postgraduate School (NPS), and a PhD in Space physics in 2018 from the University of Kansas.

Mr Dale Reding is the Scientific Advisor to the NATO Chief Scientist at NATO HQ in Brussels. In support of the Chief Scientist, he is responsible for the provision of Science and Technology (S&T) based advice to military and civilian leaders within NATO, including the study of emerging and disruptive technology trends. Mr Reding received his B.Sc. (1981) and M.Sc. (1984) in Theoretical Physics from the University of Saskatchewan. Following this, he undertook additional graduate research in Mathematical Geophysics.

Endnotes

1. 'NATO's approach to space', (2020), available at: https://www.nato.int/cps/en/natohq/topics (accessed 10 Mar. 2021).
2. Dransfield, J., 'How Relevant is the Speed of Relevance?: Unity of Effort Towards Decision Superiority is Critical to Future U.S. Military Dominance' (2020), available at: https://thestrategybridge.org/the-bridge/2020/1/13 (accessed 25 Mar. 2021).
3. The North Atlantic Treaty, art. 3, 1949.
4. Linden, D. 'The Impact of National Space Legislation on Private Space Undertakings: Regulatory Competition vs Harmonization', Journal of Science Policy & Governance, ISPG. Vol. 8. Issue 1 (2016).
5. Ibid. 3., art. 6.
6. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, art. 2, 1967.
7. Stoltenberg, J. 'NATO will defend itself' (2019), available at: https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en (accessed 20 Feb. 2021).
8. De Gouyon Matignon, L. 'The Delimitation Between Airspace and Outer Space' (2019), available at: https://www.spacelegalissues.com/the-delimitation-between-airspace-and-outer-space/ (accessed 25 Mar. 2021).
9. Ibid. 5., preamble.
10. Blount, P. J., 'Limits on Space Weapons: Incorporating the Law of War Into the Corpus Juris Spatialis' (2008), available at: https://www.researchgate.net/publication/228227466 (accessed 21 Mar. 2021).
11. Charter of the United Nations, art. 2, para. 4, 1945.
12. Ibid. 1.

© metamorworks/Shutterstock.com

Looking for a Few Good Operators

III

Opportunities for Space Force to Fulfil the Women, Peace and Security Agenda

By Dr Kyleanne Hunter
US Air Force Academy

In 2018, NATO called for the development of an overarching policy for Space, which was approved in June of 2019. Later that year the Alliance formally recognized Space as an operational domain alongside Air, Land, Sea, and Cyberspace.[1] As NATO works to craft its joint approach to the Space domain, two Allies have created military services to address it – the United States Space Force (USSF) and the French Air and Space Force (FASF). The dedicated focus on Space offers many opportunities for NATO to remain a global leader in military technology while also continuing to advance the security and stability of the North Atlantic, and, by extension, the world. Most of the focus of Space doctrine has been on the physical aspects of Space power.[2] NATO's own Space policy is currently similarly physical, focusing on how Space 'underpins NATO's ability to navigate and track forces, to have robust communications, to detect missile launches and to ensure effective command and control.'[3] However, in addition to the physical benefits to military operations that Space offers, the Space domain, including the standup of member countries' dedicated

Space-focused military services, also offer an opportunity for NATO's commitment to the Women, Peace and Security (WPS) agenda. The unique nature of the Space domain – touching and enabling operations in every other domain – provides an opportunity to meaningfully enact gendered perspectives across all operations.[4] There is an opportunity to build Space forces that accelerate the implementation of WPS to create a more secure and peaceful world. This paper discusses ways in which Space doctrine can encompass WPS tenets and how recruitment and retention policies can help NATO countries ensure meaningful leadership and operational opportunities for women.

Space as an Enabler for WPS

The Space domain touches nearly every facet of warfare. NATO presence (and arguably dominance) in Space is essential to maintain technological superiority and strategic dominance over our adversaries. Satellite technology enables Global Positioning Systems (GPS); Intelligence, Surveillance, and Reconnaissance (ISR) technology; early warning systems; and guidance for precision munitions. Indeed, a critical failure in Space would be felt in terrestrial warfighting abilities. However, the same Space-faring technologies that enable war are also essential for addressing key aspects of the WPS agenda.

A cornerstone of WPS is the fact that women and girls experience conflict and its aftermath differently than men and boys. Indeed, in many instances women suffer the most in the face of war-born resource scarcity and are often 'left behind' during conflict settlement processes.[5] While there have been attempts at codifying the importance of women's participation in the security sector, little meaningful progress has been made. For example, despite the adoption of UN Security Council Resolution 1325 in October 2000, women have participated in less than 11 % of ceasefire negotiations in the last two decades.[6] Women's exclusion from these processes result in diminished access to critical aspects of sociopolitical life that often exacerbate the cycle of conflict.[7] In addition to war and violence, climate change and the current COVID-19 pandemic are disproportionately adversely impacting women and girls, and women are similarly excluded from the processes aimed at finding meaningful solutions to these crises.[8]

The Space domain has an opportunity to address the inequalities resultant from terrestrial conflict. During- or post-conflict inequalities are often hidden, especially those that may harm women. From infrastructure damage to destruction of crops to lack of health facilities, emerging post-conflict governments often try to hide these deficiencies from the rest of the world (especially donors from Western countries).[9] However, satellite imagery can show the impact of violence in real-time – making it harder for regimes to hide atrocities.[10] Directing the use of Space technologies to highlight the plight of the most vulnerable will elevate awareness of the impact of conflict on women and girls and help direct both ground forces and government officials to places of greatest need.

In addition to recognizing (and stopping) atrocities, Space-based technology has the ability to promote gender equality in societies most likely to experience conflict. Concrete technologies such as satellite phones and mobile banking offer women independence and economic growth. Access to satellite-enabled mobile phones allows for both personal and economic independence for women, a key step towards conflict-reducing social equality.[11] Additionally, as advancements have been made in remote education technologies, Space-enabled technologies can advance women's educational attainment.[12]

Women are also often an 'early warning' signal of violence and the source of valuable human intelligence to ground forces. However, obtaining this information is often difficult for both cultural and geographic reasons.

During the conflicts in Iraq and Afghanistan, NATO nations overcame this through using women attached to combat units to directly engage with local women.[13] Yet Space allows for a more holistic participation of women in violence prevention. Evidence shows that Space-enabled satellite phone technology creates an effective early warning system for women.[14]

Filling a Personnel Gap

Newly created space forces also have the ability to impact the WPS agenda through a more meaningful and deliberate recruitment and retention of women into operational and leadership positions. Creating a doctrine that recognizes the ways in which Space technologies contribute to WPS will require recruitment and retention of diverse Space professionals.[15]

Women are quickly closing the gap in obtaining Science, Technology, Engineering and Maths (STEM) degrees, giving them the skills necessary to be operators in the Space domain.[16] Indeed, a benefit of the focused encouragement and investment in women in STEM programs worldwide is access to a robust and gender diverse workforce that has the necessary skills for the technological demands of the Space domain. Women remain largely underrepresented in NATO militaries, accounting for approximately 11 % of militaries NATO wide, falling far short of stated goals for women's recruitment.[17] Indeed, achieving success in WPS is not only predicated on advancing women's achievements abroad but also ensuring meaningful opportunities for women at home.

The creation of new Space-dedicated branches comes at a particularly unique time to achieve this. At a moment when women have the necessary skills needed to serve, both the propensity and qualifications to serve by men is on the decline. In the United States, for example, men's eligibility for service due to both education and physical fitness will decline to approximately 5 % of the population by 2040; preliminary reviews of NATO countries portend similar situations.[18]

Numerically, the stage is set to attract the diverse force that is needed to advance NATO's WPS agenda. However, to do so, these services will need to adopt new recruiting and retention programs. Traditional military services have struggled not only to recruit, but also to retain women. For nearly every NATO country, women leave the services at faster rates than men.[19] Meaningful recruitment and retention of women requires changes to personnel programs in order to address some of the key reasons women leave the services. Balancing work-family relationships and obligations are cited as one of the primary reasons that women leave the military services.[20]

Space services offer a unique opportunity to address this key issue. While Space is essential for terrestrial operations across the globe, basing for space operations can be static. The USSF is currently exploring meaningful ways to do this. In a 2020 briefing to the Defense Advisory Committee on Women in the Services, the USSF noted that flexible work schedules, dedicated engagement on diversity and seamless on-ramp/off-ramping for work in the military, academia, and industry were going to be a key part of initial personnel policies in order to maintain retention of women in the service.[21] The flexibility offered by longer dwell and geographically static basing offers an opportunity to rethink personnel policy in a way that increases the attractiveness of the service to women.

While the Space domain offers an opportunity for NATO to enable military power, it also offers a key opportunity to meaningfully advance the WPS agenda. The individuals recruited into the first cadre of Space professionals will be instrumental in creating doctrine and policies and recognize the unique role that Space can play to ensure that NATO is a leader in advancing a more peaceful world while also promoting the unique talents that women bring.

Dr Kyleanne Hunter is an Assistant Professor of Military and Strategic Studies, a nonresident fellow at the Brute Krulak Center for Innovation and Creative, and a senior adjunct fellow at the Center for New American Security. She is a retired Marine Corps Officer and former chair of the Employment and Integration Subcommittee for the Secretary of Defense's Advisory Committee on Women in the Services.

Endnotes

1. 'Key Outcomes of Summit of NATO Heads of State and Government', Brussels, Belgium 11–12 Jul. 2018, available at: https://www.nato-pa.int/download-file?filename=sites/default/files/2018-11/2018%20-%20INFO%20DOCUMENT%20ON%20NATO%20SUMMIT%20-%2014%20SESA%2018%20E.pdf (accessed 14 Mar. 2021).
2. For example, French President Macron asserts that the purpose of French Space doctrine is to strengthen the protection of French satellites for military operations (see: Reuters Staff, 'France to Create Space Command within Air Force: Macron', 13 Jul. 2019) and USSF doctrine asserts space as an instrument of power politics and military control of physical assets (see Space Capstone Publication, Spacepower. Headquarters USSF, Jun. 2020, available at https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf) (accessed 18 Mar. 2021).
3. 'NATO's Approach to Space', last updated 23 Oct. 2020, available at https://www.nato.int/cps/en/natohq/topics_175419.htm (accessed 23 Mar. 2021).
4. For an overview of NATO's approach to Women, Peace and Security see: Women, Peace and Security. Last Updated 1 Oct. 2020, available at https://www.nato.int/cps/en/natohq/topics_91091.htm (accessed 21 Mar. 2021).
5. For an overview of the differential impacts of conflict on women and girls see: Berry, Marie E., 'When "bright futures" fade: Paradoxes of women's empowerment in Rwanda.' Signs: Journal of Women in Culture and Society 41.1 (2015): p. 1–27; Kew, Darren, and Wanis-St John, Anthony, 'Civil society and peace negotiations: Confronting exclusion'. International Negotiation 13.1 (2008): p. 11–36; Kumar, Krishna, ed. Women and civil war: Impact, organizations, and action. Lynne Rienner Publishers, 2001; Usta, Jinan, and Farver, Jo Ann M., and Zein, Lama. 'Women, war, and violence: surviving the

experience', Journal of Women's Health 17.5 (2008): p. 793–804.; Ward, Jeanne, and Marsh, Mendy. 'Sexual violence against women and girls in war and its aftermath: Realities, responses and required resources.' Symposium on Sexual Violence in Conflict and Beyond. Vol. 21. 2006.

6. UN Women 'Facts and Figures: Women, Peace, and Security', available at https://www.unwomen.org/en/what-we-do/peace-and-security/facts-and-figures (accessed 10 Mar. 2021).
7. Westendorf, Jasmine-Kim, 'Peace negotiations in the political marketplace: the implications of women's exclusion in the Sudan-South Sudan peace process', Australian Journal of International Affairs 72.5 (2018): p. 433-454.
8. Arora-Jonsson, Seema,'Virtue and vulnerability: Discourses on women, gender and climate change', Global environmental change 21.2 (2011): p. 744-751; Figueiredo, Patricia, and Perkins, Patricia E., 'Women and water management in times of climate change: participatory and inclusive processes', Journal of Cleaner Production 60 (2013): p. 188–194; United Nations. 'Policy Brief: Impact of COVID-19 on Women.' 9 Apr. 2020, available at https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/policy-brief-the-impact-of-covid-19-on-women-en.pdf?la=en&vs=1406 (accessed 9 Mar. 2021).
9. For a discussion on the history of 'hiding' impacts of conflict and government policies on women see: Gates, Melinda, The moment of lift: How empowering women changes the world. Flatiron Books, 2019; Kristof, Nicholas D., and WuDunn, Sheryl, Half the Sky: Turning oppression into opportunity for women worldwide. Vintage, 2010.
10. Ó Súilleabháin, Andrea,'Shocking Satellite Photos Open New Avenues for Conflict Prevention and Response' IPI Global Observatory, 9 Apr. 2013, available at https://theglobalobservatory.org/2013/04/shocking-satellite-photos-open-new-avenues-for-conflict-prevention-and-response/ (accessed 17 Mar. 2021).
11. Porter, G., 'Mobile phones, gender, and female empowerment in sub-Saharan Africa: studies with African youth' Information Technology for Development 26.1 (2020) p. 180–193.
12. Though it is too soon to determine the impact, advancements in remote education that have been made during the COVID-19 pandemic offer an opportunity to advance women's education in conflict-impacted areas. Space technology offers the opportunity to ensure that these technologies are available in the most remote areas, further advancing NATO WPS priorities.
13. Hunter, Kyleanne, 'Shoulder to Shoulder Yet Worlds Apart: Variations in Women's Integration in the Militaries of France, Norway and the United States' (2019).
14. Luke K., 'Uses of digital technology in managing and preventing conflict', University of Manchester Report. 17 May 2019, available at https://assets.publishing.service.gov.uk/media/5d0cecb640f0b62006e1f4ef/600_ICTs_in_conflict.pdf. (accessed 14 Feb. 2021).
15. Hunter, Kyleanne, and Gaudry Haynie, Jeannette, 'The Pentagon has a plan to include more women in national security. Here's what that means and why it matters', Task and Purpose, 10 Jul. 2020, available at https://taskandpurpose.com/analysis/women-peace-security-act-dod/ (accessed 8 Mar. 2021).
16. Catalyst maintains a continually updated database of women's achievements in undergraduate and graduate degrees available at: https://www.catalyst.org.
17. Summary of the National Reports of NATO member and Partner Nations to the NATO committee on Gender Perspectives, available at https://www.nato.int/nato_static_fl2014/assets/pdf/2020/7/pdf/200713-2018-Summary-NR-to-NCGP.pdf (accessed 22 Feb. 2021).
18. Office of People Analytics, 'Updates on the Female Recruiting Market', Sep. 2018.
19. Summary of the National Reports of NATO member and Partner Nations to the NATO committee on Gender Perspectives, available at https://www.nato.int/nato_static_fl2014/assets/pdf/2020/7/pdf/200713-2018-Summary-NR-to-NCGP.pdf (accessed 18 Feb. 2021).
20. Ibid.
21. Minutes from the March 2020 DACOWITS meeting available at https://dacowits.defense.gov/Portals/48/Documents/Reports/2020/Minutes/DACOWITS%20March%202020%20QBM%20Minutes_Final.pdf (accessed 29 Mar. 2021).

© Sergey Nemirovskiy/Shutterstock.com

Avoiding Cyber Forever Wars

IV

Toward a Joint All Domain Whole of NATO Cyber Conflict Deterrence Strategy

By Ms Gentry Lane
ANOVA Intelligence

Cyberspace is poised to be the next 'forever war' battleground unless US and NATO allies change course from the current balkanized, defence-prioritized posture and enact a unilateral deterrence strategy. Cyberspace as an operational domain is rife with peculiarities that create an advantageous battlespace for adversaries. The lack of traditional visibility, ease, and efficacy in executing Offensive Cyber Operations (OCO) are favourable, especially for adversaries who prioritize stealth, persistent degradation of allied institutions in their national interest objective and wish to achieve these objectives without triggering traditional armed conflict. To disallow further adversary advancement in the Cyberspace domain, it is imperative that NATO partners accelerate agreement on desired ends, cohesive strategies, and a quantifiable framework for assessing the progress of ways and means established to deter adversary cyber aggression. The cost of inaction is too great to disregard or delay.

Cyber Conflict

For the purpose of clarity, 'cyber conflict' means aggression between Westphalian nation-state military forces with cyber combatant commands.[1] Cyber conflict can be split into two categories: peacetime aggression and wartime conflicts. (And for the purpose of this paper, 'peacetime' means any period of time outside of congressionally declared war). Unlike warfare in traditional domains, the inevitable wartime cyber conflict will not manifest as the culmination of escalating peacetime cyber aggression. Wartime cyber conflict objectives and targets will be quite different, despite indistinguishable cyber techniques, tactics, and procedures. Military Command and Control (C2) systems, transportation systems, logistics supply chains, and defence suppliers will be the high-value targets during wartime which are accessible via the Cyberspace domain. Whereas during peacetime, strategic military and intelligence assets still rank as high-value targets, but adversaries focus cyber aggression on civilian sector critical infrastructure (private-sector financial institutions, technology providers, telecom, power and water utilities, healthcare systems, etc.) and prioritize self-enrichment via industrial espionage over pure military objectives.

These peacetime and wartime military operations in the Cyberspace domain are two very different types of conflicts which require separate strategies and different theories of victory. Wartime cyber conflict will touch all aspects of the wide-ranging Joint All Domain Operations (JADO). Because of the connected character of 21st century warfare, wartime cyber conflict has the potential to compromise mission assurance at a scale previously unfathomable and never before experienced. But it is finite and limited to the duration of traditional battle, whereas peacetime cyber aggression is persistent and indefinite, the two classic characteristics of a forever war. US and allied partners are currently engaged in substantially violent peacetime cyber aggression focused on critical civilian, military, and intelligence targets. The major threat actor's salami tactics[2] of incremental degradation to critical civilian and military assets is likely a preparatory action to a forthcoming traditional armed conflict. But to relegate nation-state-perpetuated cyber aggression during peacetime to a less urgent priority is a mis-assessment of the current situation. Which cyberbattle should be prioritized: the peacetime cyber aggression currently underway or the inevitable wartime cyber conflict? To what extent are NATO allies responsible for engaging with common adversaries executing OCO primarily in the civilian sector? Or should limited resources be allocated toward preparing for wartime cyber conflict to avoid devastating, cascading consequences during battle? Without coordinated preparation for future battles, adversaries will undoubtedly pre-emptively embed in critical JADC2 systems. The Cyberspace domain provides remote access to the critical rear battle area and the ability to compromise critical JADC2 systems during battle with a proverbial single click. The NATO way of war relies heavily on joint-force interdependencies, which in turn rely on uncompromised critical digital data and communication systems. Compromise would greatly hinder NATO's force superiority.

The answer is less a matter of priority and more a matter of practicality. Can we do both? We can and we must. It is essential that NATO allies coalesce to agree upon strategy and impose conditions for conclusion to the current peacetime cyber aggression perpetuated by common adversaries, while simultaneously preparing a separate strategy for wartime cyber conflict.

Cyber conflict is a sustainable and effective form of power projection for all threat actors. The tactical asymmetry is in their favour: the cyber battlefield is pre-leveled, pitched battles are eschewed in favour of sporadic, targeted, surprise aggression, stockpiles are irrelevant, and advanced weapon systems are not required to achieve a catastrophic effect. The most advanced cyber defence technologies amount to little more than cyber – Maginot Lines that can be and are regularly circumvented. Most important, adversary cyber campaigns reliably meet national-interest objectives within an acceptable cost-benefit calculation. The escalating frequency and sophistication of nation-state cyber campaigns is proof that adversaries view their military operations in Cyberspace as advantageous. Yet bearing the brunt of the current peacetime cyber aggression is not sustainable. This begs the question, what are the opportunities for response?

A Strategy for Cyberspace

The unfortunate trend, even in erudite national security circles, is to jump directly to a discussion of cyberweapons and their tactical use. Or strategic vagaries like 'impose costs' or 'collective defence' are presented as free-standing solutions to the very complicated problem of international cyber security. Sound military-strategic logic paradigm construction begins with the ends. What is it that we want to achieve and what are the combinations of ways and means required to achieve it? Strategy is not a list of actions to undertake or an acronym-laden vision statement. A cohesive strategy is a viable, sustainable overarching concept that connects actions to resources and strengths. The connections between ways and means in a well-crafted strategy will create a self-perpetuating momentum toward the specified desired end. The ends are where NATO partners need to begin. Once an end has been established and the relevant means and ways are identified, partners can allocate resources to effectively collapse the delta between available objectives and viable objectives.

Furthermore, this resource allocation must be supported by commitment and an alignment of incentives that ensure adherence to strategy execution. Few NATO partners have fully developed cyber conflict strategies with deterrence or cessation of cyber conflict as the desired ends. No

NATO member has developed or enacted a 10-, 20-, or 100-year cyber conflict strategy, despite indicators that suggest adversaries have done so.[3]

Cyberspace as an operational domain has many idiosyncratic features, but tedious discussion is not beneficial to allied strategists at this time. Legal discussion of what constitutes homeland, violence, aggression, or an attack in Cyberspace or thresholds for engagement when there is no body count can and will ensue for years. But it does not take years for focused cyber aggression to yield impact. Every day, the major threat actors exploit allied inaction and Cyberspace domain vulnerabilities to enrich themselves, degrade economic postures and warfighting capabilities while staying below the threshold for use of (kinetic) armed force.

Conclusion

No one would deny that a sovereign nation-state has the right to pursue their national interests. And no one can deny that focused attempts to disrupt, deny, and disable critical military C2 systems via cyber effects or combatant-focused espionage and reconnaissance falls within acceptable wartime behaviour. Simply put, when national interests and behaviours conflict with LOAC (Law of Armed Conflict) or Geneva Convention protocols in any domain, the behaviour in question is unacceptable. These jus en bello violations are an excellent starting point for defining the desired ends. The Tallinn Manual is an exemplary body of work which contains a comprehensive guide to current law and cyber operations. US and NATO allies would benefit from rapid adoption of policies on which there is consensus. LOAC and Geneva Convention protocols are not warfighting domain-specific. Agreement to uphold their tenets form the basis of their power. At minimum, US and NATO allies can resolve to recognize their precedence in the Cyberspace domain, as the Tallinn Manual astutely lays out.

The force with the most effective use of cyber weapons, tactics, techniques, and procedures to achieve their desired ends, will be the victor. Victory in cyber conflict has less to do with body count or Clausewitzian ideals of defeat or surrender, and more to do with achieving strategic objectives. For the two cyber conflict scenarios under consideration, victorious ends are diametrically opposed: Adversaries benefit from under-the-radar forever wars while allies benefit from subduing adversary aggression. For allies, victory will inevitably be tied to the application and enforcement of LOAC and Geneva Convention protocols in the Cyberspace domain, unilateral OCO/DCO (Defensive Cyber Operations) capabilities and an alignment of incentives to assure commitment to achieving mutually agreed upon desired ends. It is imperative that US and NATO allies make immediate, substantial steps toward cohesive deterrence strategies to disallow further damage imposed by the major threat actors. The major threat actors need only continue in their current strategy. Unabated, they are achieving their objective.

Ms Gentry Lane is the CEO and Founder of ANOVA Intelligence, an American defence tech company, and a Visiting Fellow at the National Security Institute at George Mason University's Antonin Scalia Law School. ANOVA's groundbreaking computational approach to anomaly detection is revolutionizing cyberwarfare engagement for US companies and allies globally.

Endnotes

1. Electronic warfare operations and/or violence in the Cyberspace domain perpetuated by criminal organizations are a different problem which require different resources and strategies to address.
2. Schelling, Thomas C., Arms and Influence, 'New Haven and London', Yale University Press, 2008.
3. Scobell, Andrew; Burke, Edmund J.; Cooper, Cortez A. III; Lilly, Sale; Ohlandt, Chad J. R.; Warner, Eric; Williams, J.D., 'China's Grand Strategy: Trends, Trajectories and Long-Term Competition', Santa Monica, California: RAND Corporation, 2020.

© anttoniart/Shutterstock.com

Outer Space, a Challenging Domain for Ambitious Defence Strategy

V

Food for Thought for a Novel Space Security Diplomacy

By Dr Anne-Sophie Martin
Sapienza University of Rome

Outer Space: A Warfighting Domain

Space is vital for state security and scientific achievement. Moreover, Space-based capabilities are an integral part of our modern life and they are an essential component of nations' (or national) military power because they provide efficiency and effectiveness to military operations. However, a new schema looms with increasing rivalries between Space powers; militaries use more satellites to enhance their forces and one can observe an acceleration of the development of counterspace capabilities.[1]

Outer Space represents a strategic and operational area,[2] thus becoming a warfighting domain,[3] where states have to be able to foresee, compete, deter and respond in a challenging security environment characterized by great power competition.[4] Indeed, a diversity of actors exist, and some states such as the United States, China, Russia, and India have demonstrated that they can be ‘intimidating’ in Outer Space by conducting acts of espionage or carrying out Anti-Satellite (ASAT) tests. In fact, these inimical acts have become a reality. ASAT tests conducted by China in 2007, the United States in 2008, India in 2019 and Russia in 2020[5] perfectly illustrate this trend. In 2017, an act of espionage was conducted by a Russian satellite on Athena-Fidus, a French-Italian dual-use communications satellite.[6] It is now obvious that some states have developed systems designed to move close in order to observe and listen to Space systems of other countries, which poses serious questions in terms of security. In particular, the United States has developed a ‘Counter Communications System’ which is a deployable ground-based system that can jam signals from single satellites in geosynchronous orbit.[7] The system will allow the US Space Force to disrupt, deny, degrade, or destroy an adversary’s Space systems, or the information they provide, which may be used for purposes hostile to US national security interests.[8]

With this in mind, a sort of ‘de-sanctuarization’ of Outer Space can be observed, depicting possible new areas of conflict.[9] Currently, satellites are used to conduct military operations and Space systems have become strategic targets that can be hacked or jammed to weaken an adversary. Thus, Outer Space is becoming an environment like Cyberspace, Land, Sea or Air, where it is possible to conduct military operations.

In this new context, some states are establishing ‘Space Command Centres’, such as the United States Space Force, or the Commandement Militaire de l’Espace in France, to manage and govern Space military operations in Outer Space. Similar organization exists in Russia with the Russian Aerospace Forces,[10] in China with the Chinese programmes under the control of the People’s Liberation Army (PLA),[11] and in India.[12]

Implementation of National Space Defence Strategy: Focus on France

Outer Space is an area where state domination remains very significant, and no nation wants to be overtaken by another. Ensuring the availability of Space capabilities is fundamental to establishing and maintaining military superiority in Outer Space. In fact, states want to secure their vital interests in Space from both technological and national security policy perspectives. Indeed, they are developing new Space defence policy and strategy. For instance, France introduced in 2019 its 'Space Defence Strategy',[13] from its Ministry of the Armed Forces, outlining the notion of 'active defence' linked to the principle of self-defence. According to the strategy terms, 'active defence' means to preserve freedom of access to and action in Space, as well as to discourage any act of aggression, to detect hostile acts, and to neutralize the threat by running away, jamming, interference and dazzlement. This notion of 'active defence in Outer Space', relatively novel in European States' Space strategy, should be addressed in the framework of an international forum on Space security, and could be introduced as a new principle of international law. The French Strategy deals also with the notion of systems resilience through a distributed architecture, as well as consolidated and strengthened Space-based facilities.

New threats against Space assets and ground stations are emerging, and as a result France must reinforce its deterrence capabilities, especially against acts of spying as mentioned above. Recently, France launched a super high-resolution military satellite, CSO-2 (*Composante Spatiale Optique*), the second of the CSO constellation. The CSO military observation system brings a level of resolution and acquisition capacity unmatched in Europe, allowing France and other nations to increase their surveillance and intelligence capabilities, and France to have a greater autonomy in matters of situation assessment and decision-making.[14] For the purpose of national defence, and particularly to adapt its military Space governance, the country intends to equip its next generation of satellites, such as the Syracuse Constellation which is deployed for military communications, with cameras, machine guns and lasers, in order to identify and to tackle threats in Outer Space.[15] In addition, Space Traffic Management (STM) and Space Situational Awareness (SSA) need to be improved, especially to detect hostile acts and to defend against them.[16] Indeed, managing Outer Space requires knowledge of military actions that take place in orbit.

As of now, Space is an essential domain for the armed forces and represents a significant tool for operational support. Thus, it is of utmost importance that the French government, with the Ministry of Defence, implement a clear Space strategy in accordance with the existing international legal framework, but also by adapting its domestic legal framework to provide the armed forces with Space-operator status, allowing them to independently operate satellites.

In this context, international cooperation has to be extended between Space actors and Space operations for the purposes of the better evaluation of threats affecting Space capabilities, and to enhance military Space operations. Hence, one of the main challenges for Space security rests on the system of verification of Space technology[17] and activities in Outer Space, especially given the fact that a system should be able to detect if there is a 'militarily meaningful' violation.[18] According to a UNIDIR study, 'verifying the on-orbit actions of a Space object is easier than verifying its functions'.[19] This is particularly relevant for the development of national defence Space strategy and the issue should be further discussed within international Space security forums.

On one hand, there is a need to maintain Space autonomy and superiority, and on the other hand, the necessity to ensure Space stability in cooperation with persistent presence in Space with the objective to deter aggression and to provide for safe transit in, to, and through Outer Space. French strategy underscores the fact that novel Space missions are disrupting the existing equilibrium, and consequently, it is necessary to adapt international and domestic legal frameworks to match these new challenges. It needs to implement significant best practices and standards in order to avoid misunderstanding and misperception while conducting military operations in Outer Space.

Towards a Novel Space Security Diplomacy

With this in mind, it is necessary to reconsider Space security diplomacy within international organizations concerned with Space security, in particular NATO.[20] The principle of 'freedom of action' in case of threats in Outer Space, presented in various national Space defence strategies,[21] has to be developed in accordance with the rules of law including the five United Nations Space Treaties.[22] First, it is necessary to recall that Space activities have to be carried out in accordance with international law according to Article III of the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (OST), and that Article IV.1 of the OST does not require a complete demilitarization of Outer Space.[23] The current regime is quite permissible concerning military use of Outer Space as it does not completely forbid hostile acts.

Since there is no agreement on definitions in Space security[24] for terms including 'Space weapon', 'weapon in Space', 'threat', 'hostile intent', 'hostile act', and 'self-defence', these and some others such as 'weaponization' and 'militarization' remain ambiguously used in international debates. One of the main issues is to figure out whether a ground-based weapon directed towards objects in Space might be considered as a Space weapon. Moreover, reaching internationally acceptable definitions in the field of Space security has become more challenging with the development of new Space activities including active debris removal and satellite servicing systems, due to the nature of their dual-use core capability.[25] The emergence of new threats could compromise States' freedom of access and action. Hence, the law is not complete, but it is building gradually by taking into account the new technological development and States' practices. So, law has a significant role to play outlining terms in the field of Space security. Consequently, further discussions within the Prevention of an Arms Race in Outer Space (PAROS),[26] through the United Nations General Assembly and the Conference of Disarmament, are crucial in order to develop a common approach and harmonization in the field of Space security because States are reinforcing their military capabilities and strategies in Outer Space so as to be able to respond in case of hostile acts.

Concluding Remarks

New threats are appearing in Outer Space, and in their wake, States are developing more active and offensive Space defence strategy and policy with the aim of maintaining their autonomy and their superiority in Outer Space. In this context, it is of utmost importance to reinvent a Space security diplomacy both inclusive and collective, strengthened by norms.[27] Indeed, it is necessary to rethink Space security and collective security. Last but not least, a common understanding on the essential terms in Space security is needed in order to support the development of appropriate Space defence strategy.

Dr Anne-Sophie Martin is a Post-Doctoral Research Fellow in International Law and Space Law at Sapienza University of Rome (Italy). Her doctoral research focused on the legal aspects of dual-use satellites. She is a member of several internationally recognized institutions in the field of space law; and authors of diverse publications.

Endnotes

1. D. Porras, '2020 in Review: A Space Security Perspective', SpaceWatch GL Opinion, Dec. 2020, available at: https://spacewatch.global/2020/12/spacewatchgl-opinion-2020-in-review-a-space-security-perspective/?no_cache=1609323868; (accessed 29 Mar. 2021).
2. P. J. Blount, 'Space Security Law', Oxford Research Encyclopedias, 25 Jun. 2018, available at: https://oxfordre.com/planetaryscience/view/10.1093/acrefore/9780190647926.001.0001/acrefore-9780190647926-e-73?rskey=xzo5kM (accessed 29 Mar. 2021), see also Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain, 20 Nov. 2019, available at: https://www.nato.int/cps/en/natohq/news_171028.htm (accessed 29 Mar. 2021).
3. J. J. Klein, 'Understanding Space Strategy', The Art of War in Space, Abingdon: Routledge, 2019; Forces, US Space Force Chief: Space Is 'A Warfighting Domain', 28 Oct. 2020, available at: https://www.forces.net/news/head-us-space-force-space-warfighting-domain#:~:text=The%20head%20of%20the%20US,Space%20Operations%2C%20General%20John%20W.&text=He%20said%3A%20%22We%20didn',%2C%20but%20adversaries%20have%20evolved.%22 (accessed 19 Feb. 2021).
4. C. Steer, M. Hersch, 'War and Peace in Outer Space', Oxford: OUP, 2020; see also US Defence Space Strategy, Jun. 2020, 3 ss, available at: https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF (accessed 20 Mar. 2021).
5. The Diplomat, 'Russia Tests Anti-Satellite Missile: This is the third Russian ASAT test this year', 18 Dec. 2020, available at: https://thediplomat.com/2020/12/russia-tests-anti-satellite-missile-us/ (accessed 25 Mar. 2021).
6. DefenseNews, 'Espionage': French Defense Head Charges Russia of Dangerous Games in Space, 7 Sept. 2018, available at: https://www.defensenews.com/space/2018/09/07/espionage-french-defense-head-charges-russia-of-dangerous-games-in-space/ (accessed 21 Mar. 2021).
7. SpaceNews, 'US Space Force Declares 'offensive' Communications Jammer Ready for Deployment', 15 Mar. 2020, available at: https://spacenews.com/u-s-space-force-declares-offensive-communications-jammer-ready-for-deployment/; (accessed 29 Mar. 2021).
8. SpaceNews, 'Lockheed Martin Gets $4.9 billion Contract to Build Three Missile-Warning Satellites for US Space Force', 4 Jan. 2021, available at: https://spacenews.com/lockheed-martin-gets-4-9-billion-contract-to-build-three-missile-warning-satellites/ (accessed 18 Mar. 2021).
9. Pasco X., 'L'Espace: un Milieu Toujours Plus Conflictuel et Encombré, France Culture, 28 Feb. 2019, available from https://www.franceculture.fr/geopolitique/lespace-un-milieu-toujours-plus-conflictuel-et-encombre (accessed 12 Feb. 2021).
10. Ministry of Defence of the Russian Federation, available at: https://eng.mil.ru/en/structure/forces/aerospace.htm (accessed 12 Feb. 2021).
11. The Economic Times, 'China Attempting to Militarise Space As It Seeks to Modernise Its Military Power', 3 Aug. 2020, available at: https://economictimes.indiatimes.com/news/defence/china-attempting-to-militarise-space-as-it-seeks-to-modernise-its-military-power/articleshow/77851406.cms (accessed 18 Feb. 2021); Defense One, 'China Has a'Space Force. What Are Its Lessons for the Pentagon?', 29 Sep. 2018, available at: https://www.defenseone.com/ideas/2018/09/china-has-space-force-what-are-its-lessons-pentagon/151665/ (accessed 12 Feb. 2021); Defense News, 'China Wants to Dominate Space, and the US Must Take Countermeasures', 23 Jun. 2020, available at: https://www.defensenews.com/opinion/commentary/2020/06/23/china-wants-to-dominate-space-and-the-us-must-take-countermeasures/ (accessed 18 Mar. 2021).
12. SpaceNews, 'India Needs Its Own Space Force', 28 May 2019, available at: https://spacenews.com/op-ed-india-needs-its-own-space-force/ (accessed 24 Mar. 2021).
13. Permanent Representation of France to the Conference on Disarmament, Florence Parly Unveils the French Space Defence Strategy, 10 Jan. 2020, available at: https://cd-geneve.delegfrance.org/Florence-Parly-unveils-the-French-space-defence-strategy (accessed 24 Mar. 2021); Extrat from F. Parly's Speech, 25 Jul. 2019: 'Today, our allies and adversaries are militarizing outer space. And as the time for resilience is getting shorter and shorter, we must act. We must be ready.'
14. CSO Ministère des armées, Lancement réussi du satellite d'observation militaire CSO-2, 29 Dec. 2020, available at: https://www.defense.gouv.fr/dga/actualite/lancement-reussi-du-satellite-d-observation-militaire-cso-2 (accessed 24 Mar. 2021); see also CNES, CSO/MUSIS, 18 Nov. 2020, available at: https://cso.cnes.fr/fr (accessed 24 Mar. 2021).

15. DefenseNews, 'France Plans to Boost its Self-Defense Posture in Space', 26 Jul. 2019, available at: https://www.defensenews.com/global/europe/2019/07/26/france-plans-to-boost-its-self-defense-posture-in-space/ (accessed 24 Mar. 2021); Le Point, 'Espace: la France va armer ses prochains satellites militaires', 25 Jul. 2019, available at: https://www.lepoint.fr/societe/espace-la-france-va-armer-ses-prochains-satellites-militaires-25-07-2019-2326872_23.php (accessed 24 Mar. 2021).
16. Moro-Aguilar R. and Mirmina S.A., 'Space Traffic Management and Space Situational Awareness', in R. S. Jakhu, P. S. Dempsey (eds), 'Routledge Handbook of Space Law', Oxon, New York: Routledge, 2017, p. 180–196.
17. United Nations General Assembly Res. 75/36, Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviours (A/RES/75/36, 7 Dec. 2020), available at: https://undocs.org/en/A/RES/75/36 (accessed 24 Mar. 2021), '. . . the challenges of effectively verifying the capabilities of space objects, which can have both civilian and military applications, interpreting their behaviour or determining whether the systems will be used for purposes inconsistent with the objectives of maintaining international security and stability, while reaffirming that verification is one of the essential components of all arms control instruments . . .'.
18. D. Porras, 'Eyes on the Sky– Rethinking Verification in Space', UNIDIR, Space Dossier 4, Oct. 2019; Silverstein B., Porras D., Borrie J., 'Alternative Approaches and Indicators for the Prevention of an Arms Race in Outer Space', UNIDIR, Space Dossier 5, 26 May 2020.
19. Basely-Walker B., Weeden B., 'Verification in Space: Theories, Realities and Possibilities', UNIDIR, Disarmament Forum, vol. 3, 2010, p. 43.
20. NATO, NATO's Approach to Space, 23 Oct. 2020, available at: https://www.nato.int/cps/en/natohq/topics_175419.htm, (accessed 10 Mar. 2021).
21. For instance, the US Defense Space Strategy, Jun. 2020, available at: https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF (accessed 12 Mar. 2021).
22. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27 Jan. 1967, 18 UST. 2410, 610 U.N.T.S. 205; Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, 18 Dec. 1979, 18 I.L.M. 1434, 1363 U.N.T.S. 3; Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, 3 Dec. 1968, 19 UST. 7570, 672 U.N.T.S. 119; Convention on International Liability for Damage Caused by Space Objects, 29 Mar. 1972, 24 UST. 2389, 961 U.N.T.S. 187; Convention on Registration of Objects Launched into Outer Space, 12 Nov. 1975, 28 UST. 695, 1023 U.N.T.S. 15.
23. Ribbelink O., Article III, in S. Hobe, B. Schmidt-Tedd, K. U. Schrogl, CoCoSL, vol. I, Köln: Carl Heymanns Verlag, 2009, p. 64–69; K. U. Schrogl, J. Neumann, Article IV, in S. Hobe, B. Schmidt-Tedd, K. U. Schrogl, CoCoSL, vol. I, Köln : Carl Heymanns Verlag, 2009, p. 70–93 ; see also F. Lyall, P. B. Larsen, Space Law A Treatise, Oxon, New York: Routledge, 2018, 447 ss.
24. Sa'id Moteshar, Space Law and Weapons in Space, Oxford Research Encyclopedia, 23 May 2019, available at: https://oxfordre.com/planetaryscience/view/10.1093/acrefore/9780190647926.001.0001/acrefore-9780190647926-e-74 (accessed 20 Mar. 2021)
25. Martin A. S., 'Studi sugli Aspetti Giuridici dei Sistemi Satellitari Duali', Strategie Spaziali Presenti e Future, 2019, Beau Bassin: EAI.
26. Masson-Zwaan T., Hofmann M., 'Introduction to Space Law, Alphen: Wolters Kluwer', 2019, p. 69–71; see also A.S. Martin, Forty Years of Negotiations on PAROS: Outcomes and New Challenges, SpaceWatchGL Opinion, Nov. 2020, available at: https://spacewatch.global/2020/11/spacewatchgl-opinion-forty-years-of-negotiations-on-paros-outcomes-and-new-challenges/ (accessed 20 Mar. 2021).
27. Ibid.17., '. . . the need for all States to work together to reduce threats to space systems through the further development and implementation of norms, rules and principles of responsible behaviours with the aim of maintaining a peaceful, safe, stable, secure and sustainable outer space environment, which might, as appropriate and without prejudice, contribute to further consideration of legally binding instruments in this area . . . '.

© stockwerk-fotodesign/Shutterstock.com

Increasing NATO's Resilience

VI

Soft Power as a Countermeasure to Hybrid Threats

By Mr Omree Wechsler and Mr Doron Feldman
Tel Aviv University

Amidst the COVID-19 pandemic outbreak in Europe, several state-led disinformation campaigns were launched in NATO's member states with the goal to undermine the public support in the Alliance and deepen the divisions between allied nations. NATO's military components, such as Air capabilities, may be part of a comprehensive strategy to counter the threat.

Hybrid Warfare and Disinformation: NATO's Soft Underbelly?

While not quite a new phenomenon, hybrid warfare has been discussed in international forums since the Russian annexation of Crimea in 2014.[1] However, since its outbreak, the COVID-19 pandemic has witnessed a surge in disinformation campaigns and attempts to control and sow false narratives, many of which targeted NATO with the aim of undermining public support in the Alliance and deepening the divisions between its member states. In March 2020, Lithuanian media outlets reported that their content management systems were hacked and that a false story accusing NATO soldiers of spreading the pandemic in the country appeared on their websites.[2] In July 2020, security firm FireEye's subsidiary, Mandiant, released a report on a disinformation campaign named Ghostwriter, the aim of which was to undermine NATO and US troops in Poland and the Baltics by leveraging anti-US narratives and themes related to the pandemic.[3]

According to the Commander of US Cyber Command and Director of the NSA, General Paul Nakasone, the low cost of foreign influence operations, facilitated by easy and high exposure to social media users make them attractive to adversaries to spread discord while operating below the threshold of armed conflict.[4] Given that hybrid threats and disinformation campaigns have become the 'weapon of choice' for NATO's adversaries, and that the Alliance's cohesion, legitimacy, and public trust are growing more critical in the face of global crises, NATO should turn to alternative approaches in order to improve its resiliency and capability to respond to future crises.

This paper suggests a soft power approach to preserve the Alliance's legitimacy and cohesion and promote further cooperation with member and non-member states.

NATO's Approach to Counter Disinformation

In July 2018, NATO's member states recognized hybrid threats and disinformation as a challenge to the stability of the Euro-Atlantic security environment.[5] NATO's approach to countering disinformation includes tracking, monitoring and analyzing the information environment relevant to its missions and tailoring its strategic communications in order to deliver fact-based, timely, transparent, and coordinated information. In order to do so, NATO has intensified its digital communications on the pandemic response across all platforms, turned public diplomacy events into online engagements and enhanced the dissemination of communications in the Russian language. NATO has also increased the support for think tanks, fact-checking organizations and other civil society initiatives in order to promote debate and build resilience.[6]

However, research has shown that disinformation spreads faster and has a greater reach than verified facts[7] and spreads even faster during crises, such as pandemics.[8] These conclusions may render NATO's approach less effective due to the strategic time gap between the spread of disinformation and the response to it.

A suggested long-term solution, which could help the Alliance to utilize its military components in order to maintain its image, attraction and public support, is a comprehensive soft power strategy.

A Soft Power Strategy: NATO's Missing Component?

Soft power describes a country's ability to persuade others to change their behaviour without force or coercion. It arises from the attractiveness of a country's culture, political values, and policies.[9] Exercising soft power domestically can increase resilience, social cohesion, solidarity, trust, legitimacy, and the central government's attractiveness.[10] Over time, the concept of soft power has come to apply to various actors in world politics, including Intergovernmental Organizations (IGOs).[11]

Over the years, utilizing military components in order to project soft power was termed 'military diplomacy'. Military diplomacy refers to the pursuit of foreign policy objectives through the peaceful employment of defence resources and capabilities, such as disaster relief and medical and humanitarian aid operations.[12] In this sense, a swift and timely response to global or regional crises could contribute to NATO's soft power strategy. Since the COVID-19 outbreak, NATO has conducted numerous airlifts of medical supplies, built dozens of field hospitals and provided thousands of beds and logistic assistance to international organizations through the Euro-Atlantic Disaster Response Coordination Centre (EADRCC).[13]

However, as a military organization, NATO's ability to respond to medical emergencies is limited and response is largely dependent on its member states' initiatives. Limiting NATO's role in responding to a non-military crisis has led to a delayed response based on differing perceptions of the threat among its member states, which China and Russia have exploited for propaganda purposes.[14]

Strategically, NATO should strive to use its logistical apparatus, command and control structures, and its connections on both sides of the Atlantic in order to increase and maintain its readiness and responsiveness to future civilian emergencies. This will showcase increasing relevance, effectiveness, and the ability to adapt to changing strategic circumstances, all of which are crucial for the establishment of a soft power strategy.

NATO's Air Power Capabilities: Current Initiatives and the Risks for the Future

A major component of a soft power strategy, which builds upon NATO's ability to respond in a timely and coordinated manner to civilian crises such as pandemics, relies heavily on leveraging NATO's Air Power, and more specifically, its airlift capabilities. NATO's strategic airlift capabilities rely on several Alliance-supported initiatives such as the Strategic Airlift

International Solution (SALIS) that enables participating allies to charter commercial transport aircraft, and the Strategic Airlift Capability (SAC), through which participating allies jointly own and operate C-17 Globemaster III heavy cargo aircraft.[15] Two other initiatives expected to significantly increase European airlift capabilities are the European Air Transport Command's (EATC) program for its seven-member nations to jointly purchase and operate Airbus A400M aircraft, and the developing Multinational Multi-role Tanker-Transport Unit (MMU) comprised of eight Airbus A-330 aircraft collectively purchased and operated by six NATO nations.[16]

However, these initiatives seem to be scattered and are not under control of NATO. Furthermore, these initiatives face risks that derive from changes in the strategic environment such as sudden security emergencies, further deployment to other theatres etc.

Moreover, NATO's airlift capabilities still rely heavily on US strategic airlift while other member states suffer a severe gap in requirements and capacity.[17] Despite earlier expectations that the A400M fleet initiative would mitigate gaps in European airlift capability, the program has been facing technical and cost challenges and delays.[18] Due to the delays, European member states will have to continue their reliance on the SALIS initiative, designed as an interim solution, until agreement on a long-term procurement solution.[19]

Furthermore, these gaps may worsen due to the changing strategic environment. During the first months of the pandemic outbreak, these initiatives have been vital to the prompt delivery of humanitarian and medical aid.[20] However, given the current state, a combination of scenarios could potentially strain and wear NATO's existing airlift capabilities. These scenarios include a resurgence of the COVID-19 crisis due to the emergence of new, potentially deadlier and vaccine-resistant variants of the virus, along with provocations along the Alliance's Eastern Flank, and predicted overall cuts to defence spending.[21] To maintain its ability to fulfil its missions amidst heightened crisis scenarios, NATO will have to expand its access to strategic airlift capabilities.

Expanding NATO's Airlift Capabilities: A Suggested Solution

While acquiring airlift capabilities seems like an obvious solution, purchasing transport aircraft is a long and expensive process. Therefore, a suggested solution for increased access to airlift capabilities during crisis should focus on collective contracting. However, unlike SALIS, which since 2018 relies on Antonov Logistics Salis as a single provider, a new solution should involve contracting several commercial airlines through member states' militaries in order to allow rapid and flexible access to airlift for different requirements and changing scenarios. Such a solution already exists as part of the US Civil Reserve Air Fleet, through which US airlines voluntarily commit, by contract, to support US Department of Defense airlift requirements in times of emergencies. While ideas to establish a NATO equivalent in Europe began in the 1970s, only a few European member states supported the idea.[22] However, with NATO's member states almost doubled since the 1970s, along with new partner states and with a clearer understanding of NATO's potential contribution in times of a civilian or a medical emergency, this idea is due for a revisit and reconsideration. However, difficulties to deploy airlift capabilities for certain contingencies are likely to remain. This is due to the veto right given to each member state. To address this difficulty, NATO should discuss pandemics and natural disasters under the Article 3 resiliency criteria. Article 3 directs member states to develop and maintain their capacity to resist major shocks, such as armed attacks or natural disasters, by means of self-help and mutual aid. One of the article's basic requirements is resilient transport systems to ensure the rapid movement of NATO's forces across the Alliance territory.[23] Enlarging the Alliance's access to flexible airlift solutions would strengthen its ability to deliver humanitarian aid and offer disaster relief as part of projecting its soft power, thus allowing it to mitigate threats to its cohesion, solidarity and public support.

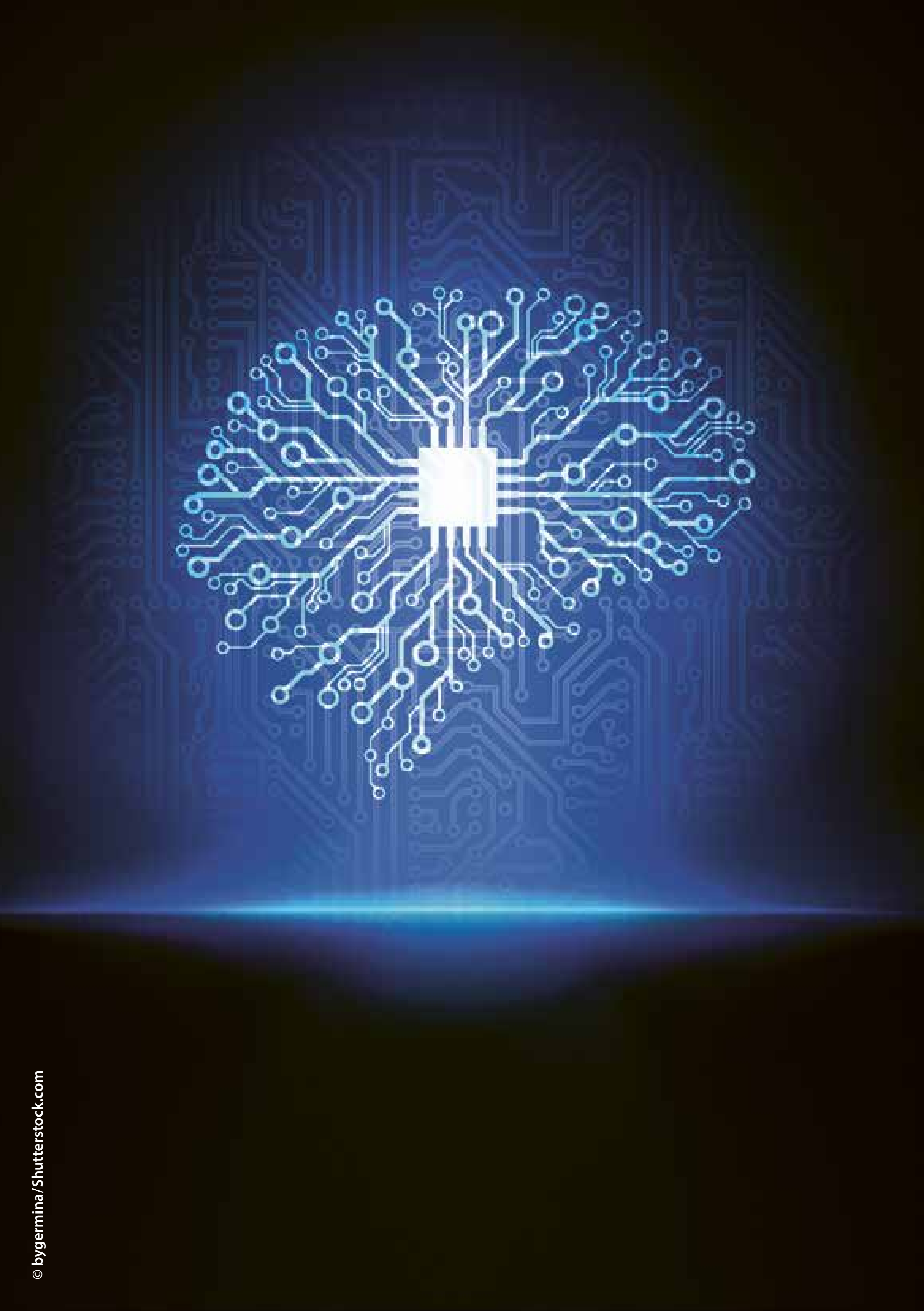
Mr Omree Wechsler is a senior researcher for cybersecurity policies and strategy at the Yuval Ne'eman Workshop for Science, Technology and Security in Tel Aviv University. His research fields include information operations, elections cybersecurity, national cyber strategies, cyber threats on space systems and cyber weapons proliferation.

Mr Doron Feldman is a PhD. candidate in the Doctoral Students Program in The School of Political Science, Government and International Affairs at Tel-Aviv University. His research focuses on the national security strategies of small nations that live in a conflict environment and their soft power implementation.

Endnotes

1. Marović, J., 'Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation,' in 'New Perspectives on Shared Security: NATO's Next 70 years.' Carnegie Europe, https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419#tableContents, Nov. 2019 (accessed 12 Jan. 2021).
2. Tucker, P., 'Russia pushing Coronavirus lies as part of anti-NATO influence ops in Europe,' DefenseOne, https://www.defenseone.com/technology/2020/03/russia-pushing-coronavirus-lies-part-anti-nato-influence-ops-europe/164140/, 26 Mar. 2020, (accessed 13 Jan. 2021).
3. Mandiant, 'Ghostwriter' Influence Campaign,' https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf, Jul. 2020 (accessed 13 Jan. 2021).
4. Vavra. S., 'NSA director ranks influence operations as a top concern,' CyberScoop, https://www.cyberscoop.com/nsa-director-nakasone-influence-operations/, 16 Sep. 2020 (accessed 13 Jan. 2021).
5. NATO, Brussels Summit Declaration: Issued by the Heads of State and Government participation in the meeting of the North Atlantic Council in Brussels 11–12 Jul. 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm (accessed 13 Jan. 2021).

6. NATO, NATO's approach to countering disinformation: a focus on COVID-19, https://www.nato.int/cps/en/natohq/177273.htm, 17 Jul. 2020 (accessed 13 Jan. 2021).
7. Dizikes, P., 'Study: On Twitter, false news travels faster than true stories,' MIT News, available at: https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308, 8 Mar. 2018 (accessed 15 Jan. 2021).
8. Depoux, A., Martin, S., Karafillakis, E., Preet, R., Wilder-Smith, A., & H.J. Larson, 'The pandemic of social media panic travels faster than the COVID-19 outbreak,' Journal of Travel Medicine, vol. 27, no. 3 (Apr. 2020), available at: https://doi.org/10.1093/jtm/taaa031 (accessed 13 Feb. 2021).
9. Nye, J. S., 'Soft Power: The Means to Success in World Politics', New York: Public Affairs, 2004.
10. Wang, L., & Y. C. Lu, 'The Conception of Soft Power and Its Policy Implications: a Comparative Study of China and Taiwan', Journal of Contemporary China, vol. 17, no. 56 (2008): p. 425–447.
11. Smith, K. E., 'Is the European Union's Soft Power in Decline?', Current History, vol. 113, no. 761 (2014): p. 104–109.
12. Pajtinka, E., 'Military Diplomacy and its Present Functions,' Security Dimensions. International and National Studies, no. 20, 2016, p. 179.
13. NATO, NATO's response to the COVID-19 pandemic factsheet, available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/11/pdf/2011-factsheet-COVID-19_en.pdf, Nov. 2020 (accessed 20 Jan. 2021).
14. De Maio, G., 'NATO's response to COVID-19: Lessons for resilience and readiness,' Brookings, Oct. 2020, p. 3, https://www.brookings.edu/wp-content/uploads/2020/10/FP_20201028_nato_covid_demaio-1.pdf (accessed 20 Jan 2021); Brzozowski, A. 'NATO tells top commander to speed up medical aid in response to pandemic,' Euractiv, https://www.euractiv.com/section/defence-and-security/news/nato-tasks-top-commander-to-speed-up-medical-aid-in-response-to-covid-19-pandemic/, 3 Apr. 2020 (accessed 20 Jan. 2021).
15. NATO, Strategic Airlift, available at: https://www.nato.int/cps/en/natohq/topics_50107.htm, 13 Oct. 2020 (accessed 24 Jan. 2021).
16. NATO Support and Procurement Agency (NSPA),14 May 2020, available at: https://www.defense-aerospace.com/articles-view/release/3/211246/european-mmf-tanker-pool-to-receive-first-two-aircraft-in-june.html#:~:text=The%20Multinational%20Multirole%20Tanker%20Transport%20Unit%20%28MMU%29%20The,Forward%20Operating%20Base%20%2B%20%28FOB%2B%29%20in%20Cologne-Wahn%20%28Germany%29 (accessed 29 Mar. 2021).
17. Hages, L., 'Europe's strategic airlift gap: Quantifying the capability gap and measuring solutions,' JAPCC Journal 19 (2014): pp. 21–25; Efstathiou, Y., 'European Strategic Airlift: a Work In Progress,' International Institute for Strategic Studies, available at: https://www.iiss.org/blogs/military-balance/2019/01/european-strategic-airlift#, 10 Jan. 2019 (accessed 22 Jan. 2021).
18. Pfeifer, S., 'Airbus agrees revised deal for troubled A400M programme,' Financial Times, https://www.ft.com/content/ed8682bc-8ea0-11e9-a24d-b42f641eca37, 14 Jun. 2019 (accessed 24 Jan. 2021); Meyer, D. 'Airbus's A400M was meant to be the pride of Europe's military. But after years of problems it still has a screw loose,' Fortune, https://fortune.com/2019/11/14/airbus-a400m-loose-screw-germany-luftwaffe/, 14 Nov. 2019 (accessed 24 Jan. 2021).
19. Ibid. 15.
20. Ibid. 14., p. 5.
21. Morcos, P., 'Toward a New "Lost Decade"? COVID-19 and Defense Spending in Europe',Center for Strategic and International Studies, Oct. 2020, p. 2, available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201015_Morcos_Toward_Lost_Decade.pdf (accessed 24 Jan. 2021).
22. Crackel, T. J., 'A History of the Civil Reserve Air Fleet.' US Air Force History & Museums Program [website], 1998, p. 178, available at: https://media.defense.gov/2013/Sep/16/2001329866/-1/-1/0/AFD-130916-006.pdf (accessed 24 Jan. 2021).
23. NATO, Resilience and Article 3, available at: https://www.nato.int/cps/en/natohq/topics_132722.htm, 16 Nov. 2020 (accessed 5 Mar. 2021).



© bygermina/Shutterstock.com

Dynamic C2 Synchronized Across Domains – Panel Introduction

VII

By Maj Osman Aksu, TU Air Force
Joint Air Power Competence Centre

Introduction

In a world of greater competition, future peer adversary capabilities, including the threat posed to Alliance platforms from Air defence systems, will continue to develop and increase in lethality at a relentless pace. The concept of uncontested operating environments has been replaced by the new paradigm of a contested environment defended by adversary Anti Access Area Denial (A2/AD) capabilities. NATO must adapt to this new norm and acknowledge a new threat environment where 'speed' is crucial. The pivotal question now is how do Alliance military preparations and operations need to adapt to effectively respond to these evolving threats, while simultaneously ensuring the risks remain manageable and NATO's limited resources used synergistically, efficiently, and effectively to provide Air and Space Power at the Speed of Relevance. Alliance commanders will be asked to make effective responses to the operational environment's broad range of challenges and address future dynamic conflicts with a new mindset.

Decision-making and dynamic targeting cycles will be conducted with limited time and information. These conditions will greatly disturb the traditional Command and Control (C2) dynamics. To increase the speed of decision-making of joint forces' C2 and to increase survivability in the battlespace against peer adversaries' threats, the Alliance will require synchronized, interoperable, and resilient C2 structures across all domains. Without changing the basic principles of C2, new technologies and their associated change to operational dynamics are needed to harmonize the Alliance C2 structure. Some of these new technologies include enhanced satellite communications technologies, Artificial Intelligence (AI), Machine Learning (ML), Big Data Management, modelling of Human-On-the-Loop, Human-In-the-Loop, and Human-Out-Of-the-Loop through command cycles, and digital connectivity features. There also exists a requirement for well-trained personnel grounded in the fundamental C2 concepts to harmonize the Alliance C2 structure. In this context, while this panel aims to present a different perspective on the basic issues presented above, it also aims to sketch out a roadmap for what to do in the NATO C2 Concept for the upcoming development period.

Transitioning to a New Era of C2

The NATO 2030[1] initiative assesses the main trends that will shape NATO's environment between now and 2030. It outlines that NATO's external security environment has changed dramatically since 2010, and in this emerging decade of renewed systemic rivalry and growing transboundary threats and risks, highlights that a functioning and robust NATO military command structure will be more important to the security of Alliance.

Additionally, NATO's Strategic Foresight Analysis (SFA)[2] provides a predictive view of the world's strategic trends out to and beyond 2035; it presents a vision of political, social, technological, economic, and environmental trends. It concludes that asymmetric conflict scenarios will continue and surmises that the need for collective defence against a peer or near-peer adversary will increase. It also points out that to keep our military edge, prevail in future operations and to face peer and near-peer opponents in all domains, Alliance forces will need resilient, adaptable and interoperable C2 systems to provide awareness and a 360-degree, 24/7 operational picture, across all domains. It also suggests that we will require the ability to overcome A2/AD environments and hybrid threats.

Today's military operations are becoming more complicated with the rise in the number and variety of commanders' options at all levels of the organization. The expansion of military activity beyond the Air, Sea, and Land domains to Space and Cyberspace has broadened the community of warfighters that modern militaries require to operate successfully and efficiently in the battlespace. As the changing character of war becomes enmeshed in the digital age, future conflicts will be decided by those who are the fastest at collecting, correlating, fusing, analyzing, and securely transporting the right decision quality data across multiple domains to the appropriate decision-maker.[3] Having the ability to operate in all domains creates more vital opportunities for commanders to employ their forces strategically against peer adversaries. However, this ability requires interoperability and the detailed integration of all domains. Often, much of the available data is not relevant to most users. There must be some guidelines on who gets what information. Information technology must enable the decision-maker in the future to access high-quality information, which is relevant at a specific moment in time and to his or her specific position within the C2 organization. C2 is not just about situational awareness, it is also about how and by whom decisions are made. Dynamic, real-time information sharing and networking are critical for establishing full operational capabilities and facilitating these exchanges. Simultaneously, multiple-domain or all domain operations create additional command and control load and bring responsibilities such as training, education, manning, and require institutionalizing policies by their nature.

Perhaps the only way to eliminate such problems before they arise is to strengthen jointness across all domains and services. Traditionally, the concept of **Jointness** is defined as different fighting services that are working with and supporting each other. Another point of view regarding Jointness is that 'Jointness is not created by doctrine, joint or otherwise. It is brought about by people, good and bad. Like most things in life, it is created more successfully by having a higher proportion of professional people well trained in their service capabilities and how to employ them.'[4] The intent is to at least provide 'Jointness' in concepts, organizational constructs and training.

One of the new approaches for this purpose is Joint All Domain Command, and Control (JADC2). Joint All-Domain Operations (JADO) are those actions taken by the joint forces of two or more NATO nations, comprised of all appropriate domains, integrated in planning and synchronized in execution, at a pace sufficient to effectively accomplish the mission.[5] To win future battles, the side with an information advantage across multiple domains will undoubtedly have decisive advantages. It is essential to ensure that the right information is available to the right decision-maker at the right place and time. A resilient JADC2 architecture would enable commanders to understand the battlespace more rapidly, direct forces faster than the peer adversary, and deliver synchronized combat effects across multiple domains.[6]

Legacy C2 Dependency

C2 tasks traditionally include establishing the command hierarchy, authority allocation and delegation, planning, allocating resources, assigning, and managing functions through mission objectives. Occasionally, military decision-makers are dependent on legacy C2 systems impeded by multiple barriers, including those between classification levels, separate services, and Alliance capability disparities. In addition, the accelerated emphasis on improved Cyberspace and Space integration has placed new functional and technical demands on C2 systems. Synchronization at the speed of decision-making and timing is sometimes challenging, if not impossible. This C2 dependency could be minimized by developing new technologies, fielding new capabilities and enhancing interoperability between services and nations. New technologies should be pursued, especially for use in contested environments, to make the communications chain and data exchange more resilient. Sometimes, other than the technological mitigations for challenged C2, the next best option might be to find procedural and organizational mitigations to cover the technical shortcomings and execute distributed control of critical missions when required. The transition of operations from uncontested to contested environments and the preparation for high-end conflicts against peer adversaries has created the need to change the highly centralized C2 of Air operations. Creating more C2 nodes and handing over more responsibilities to subordinates via mission-type orders can help achieve the commander's intent in contested environments. A mobile and robust adversary and its highly resilient assets will characterize the contested battlespace environment of the future. These conditions create a need to increase the scale of information processing. The combination of imminent threats to the joint force, the limited time of battlespace access due to area denial systems, and the increased use of standoff weapons will shorten the decision time available. The current C2 of the dynamic targeting construct is not adequate to achieve the speed of tactical decisions required in this operational context. Allies should explore flexible C2 models that will allow for the maximum amount of effective decentralization.[7]

Those options require significant changes in the traditional approach to C2, including renovating the organizational structure, qualified manning and assignments, training, and leveraged C2 technologies. However, in the time-constrained and contested environment, the target-strike decision might need to be made closer to the source of target detection, like from an Unmanned Aircraft System (UAS), with the help of subordinate Tactical Command and Control (TAC C2). Planners should explicitly clarify the delegation of authority and the degree of control before establishment of the mission plan and execution of operations.

The design of distributed C2 should be based on an analysis of risk factors, such as feasibility, inefficiencies, costs, resources, and threats by peer adversaries. Whatever the implementation, various investments in new technologies and practices will be necessary to evolve from centralized C2 physical centres. AI/ML can help enable this shift to distributed control, for example, by providing predictive tools (e. g., for force readiness at a wing operations centre), dynamic courses of action generation at a subordinate node, and decision tools for commanders at forward operating nodes.[8]

Additional Articles

This section presents five related articles which will introduce various ideas and perspectives related to the dynamic C2 synchronized across domains and the current challenges NATO faces therein. The ideas expressed in these articles are meant to inspire critical thinking to prepare those attending the 2021 Joint Air & Space Power conference for the panel discussion Dynamic Command and Control Synchronized across Domains:

- Lieutenant General Fernando De La Cruz Caravaca (SP Air Force) provides a senior leader's perspective on the idea of ***Dynamic C2 Synchronized Across Domains***. As the Commander of the NATO Combined Air Operation Centre – Torrejón, he provides unique insights into the current environment, discusses new technologies and threats, and shares his thoughts on multi-domain C2, dynamic and synchronized.

- In ***Is Human-On-the-Loop the Best C2 Architecture to Deliver Rapid Relevant Responses (R³)?***, Dr Michael Cowen, Captain (ret.) Rick Williams (US Navy), and Brigadier General (ret.) Doug Cherry (US Army) discuss the comparison between Human-On-the-Loop, Human-In-the-Loop, and the progression to Human-Out-Of-Loop. The paper also discusses the supervisory control capabilities, requirements, and issues implicit in each human in/on/out of the loop architecture to safely deliver Rapid Relevant Responses (R^3) as cycle time approaches zero to reduce the probability of a robot war incident.

- The next paper ***Technology and Connectivity: an essential bond for a modern Air Force*** is written by Major Ferdinando Pagano (IT Air Force). This paper focuses on modern Air Power challenges and complexities and the linkage between technologies and digital connectivity to operate efficiently across all domains.

- Colonel (ret.) Hubert Saur's (GE Air Force) ***Multi-Domain Combat Cloud – A Vision for the Future Battlefield*** appears next in the booklet. The paper articulates that future warfighting will require a far higher degree of processing, automation, and integration throughout the Mission Cycle. To tackle these challenges, this paper argues on behalf of a Multi-Domain Combat Cloud solution to enable forces to Be Informed as One and Act as One.

- This topic ***NATO Command and Control Resilience in Contested Environments*** by Ms Clementine G. Starling and Mr Owen J. Daniels presents the ongoing C2 challenges for NATO and possible approaches for improving C2 resiliency. The paper goes into JADC2 concept, and how or why NATO Allies consider similar concepts to bolster combat effectiveness, ensure integration, and maintain interoperability against degraded C2.

- ***Human-On-the-Loop*** is a collaborative work by Colonel (ret.) Thomas Vincotte (FR Air Force), Brigadier General (ret.) Jean Michel Verney (FR Air Force), and Mr Laurent le Quement. This paper discusses new innovative technological approaches where software, artificial intelligence, automation, and satellite communications will bypass human limitations. The paper also touches upon a strong link that exists between the amount of information to be processed, the tempo, and the position of humans in the decision process.

Major Osman Aksu (TU Air Force) holds a Bachelor of Electronic Engineering Degree from the Turkish Air Force Academy in 2001. He had basic Weapons Controller (WC) training until 2003 in İzmir. He worked as a WC at Diyarbakır CRC until 2008, selected as AEWC Project Officer in US and TUAF HQ until 2013, assigned as Airspace Coordination Officer in ATC Ankara between 2014 and 2019. He participated in Airspace Control-Management activities for US/Coalition Operation Inherent Resolve missions.

Endnotes

1. R. Group, NATO 2030: United for a New Era, 2020.
2. NATO Supreme Allied Commander Transformation (SACT), Strategic Foresight Analysis, 2017.
3. NATO Supreme Allied Commander Transformation (SACT), NATO's Joint Air Power Strategy (JAPS) Interoperability Study, NATO Supreme Allied Commander Transformation, 15 Jan. 2020.
4. L. B.Wilkerson, 'What exactly is Jointness,' Joint Force Quarterly: JFQ, no. Institute for National Strategic Studies, National Defense University, p. 66, 1996.
5. Joint Air Power Competence Centre,' https://www.japcc.org,' Mar. 2021. Available at: https://www.japcc.org/publications/?term=6&orderby=date&order=DESC.
6. Nishawn S. Smagh, 'Defense Capabilities: Joint All Domain Command and Control,' Congressional Research Service (CRS), 6 Apr. 2020.
7. N. J. Hall, 'Preparing For Contested War: Improving Command And Control Of Dynamic Targeting,' USAF, Air University.
8. Sherrill Lingel, Jeff Hagen, Eric Hastings, Mary Lee, Matthew Sargent, Matthew Walsh, Li Ang Zhang, David Blancett, 'Joint All-Domain Command and Control for Modern Warfare', Santa Monica, California: RAND Corporation, 2020.

© greenbutterfly/Shutterstock.com

Dynamic C2 Synchronized Across Domains

VIII

Senior Leader Perspective

By Lt Gen Fernando De la Cruz Caravaca, SP Air Force
Commander, NATO Combined Air Operation Centre Torrejón

The Current Environment

Since the end of the last century, we have witnessed new forms of crises appearing around the world both close to, and sometimes within, NATO territory. These events have the potential to rapidly evolve and escalate with little warning, making them difficult to predict and prepare for as an Alliance. The scope of these non-traditional threats can be broad and include the use of unsophisticated weaponry, such as dirty bombs, and non-kinetic capabilities, such as cyberattacks, which requires us to be perpetually prepared. In these scenarios, it is our ability to promptly recognize indications and generate warnings that allows us to effectively respond to a potential problem, risk, or adversary.

In addition, the pace and scope of technological advancements and the use of new forms of communication have changed the societal mindset and altered the military's approach to conflicts, affecting the way operations are planned and executed. Other factors are increasingly fundamental in the planning of current military operations such as Rules of Engagement (ROE) and the use of non-kinetic capabilities in the so-called 'grey zone' which plays into the broader strategic communications concept. Furthermore, we must consider new domains in addition to traditional ones, such as Space or Cyberspace. These complex operational domains are becoming increasingly contested and congested and can have a significant impact on military operations.

More so than ever before, actions carried out in one domain have the potential to affect the others, so it is necessary to plan and act across all of them. The planning and conduct of military operations must be coherent and carried out from the point of view of the multi-domain concept. Therefore, to achieve positive results, it is important to work in a synchronized and coordinated manner in all domains, unifying all efforts and being able to adapt to changes as they appear. In this way, we can prevent activities in one domain from interfering negatively with those in another and hence we must be able to work effectively in a multi-domain Command and Control (C2) structure. To do so, it is necessary to have the right tools, training, and the mentality to act in dynamic, challenging scenarios. Only in this way can we address the ever-increasing complexity of current crises or conflicts.

New Technologies, New Threats

Rapid technological advancements have created new possibilities for operations across all domains. Additionally, the development of new weapons systems (unmanned vehicles, fifth-generation aircraft, precision-guided munitions, hypersonic armament, non-kinetic weaponry, etc.) along with sophisticated tools for command and control (satellites, radar, communication systems, and secure, high-speed data links) have brought increased risks and challenges for which we must be prepared.

The impressive progress in processors, computer systems, and data management allows an immense amount of data to be processed automatically, analysed in record time, and converted into useful information (Big Data). The increased use of 5G will also improve the capability of systems to handle greater data processing, which will increase the ability to exploit Big Data and to disseminate information to optimize decision-making.

Advancements in the use of Artificial Intelligence (AI) and Machine Learning (ML) necessitate new skill-sets and will create new specializations. Processes will become either fully automated and performed by machines or robots (Human Out of the Loop (HOOTL)) or will continue to require human input and decision-making (Human in the LOOP (HITL)), or at least Human approval of decisions (Human On the Loop (HOTL)). For example, the management and analysis of intelligence data collected consumes a great deal of time and human resources to process all the available information. Technology can provide a system capable of merging the different formats in which the data is collected, facilitating the integration of multi-domain intelligence tools from different sources (electro-optical, infrared, radar, acoustic, and signal) and from different domains (Land, Sea, Air, Cyberspace, or Space).

Thanks to emerging technologies, the potential role of the autonomous robot on the future battlefield is increasing. For example, cyber-bots can be used to target enemy information systems and autonomous vehicles can conduct minefield clearance to facilitate logistics convoys, thus removing humans from danger zones. Those activities that are functional, repetitive, and life-threatening could be more automated, thereby freeing up capacity for the human element to be prioritized elsewhere.

Technology also offers the potential to use tools such as 'Federated Mission Networking' or to expedite the Process Exploitation and Dissemination (PED) of information between domains. These characteristics underpin a secure C2 network which protects the integrity of our information and preserves the ability to effectively process, share and exploit data on the battlefield. This can help us address some of our most important operational challenges such as defeating 'Anti-Access/Aerial Denial' systems.

Big Data and AI can automate many of these processes, accurately streamline the analysis of the data obtained and assist in rapid decision-making. This, in turn, saves ever more scarce human resources and allows them to be dedicated to other activities. Also, simulation processes across all domains can facilitate effective decision-making and for that reason they are very useful tools for C2.

However, we must be wary of an over-reliance on all these tools as they can make us very much dependant on technology; this could leave our systems, and hence our operations, susceptible to cyber-attacks. Therefore, it is imperative to develop a cybersecurity strategy that protects our key vulnerabilities and ensures our resilience.

Multi-Domain C2 and Dynamic Synchronization

An effective C2 structure must be able to synchronize activities across all domains in order to deal with evolving threats. It must be able to exploit the full range of capabilities and yet decision-makers must remain aware of the potential effects that an action taken in one domain may have on another. At the same time, a C2 structure must be dynamic enough to respond to any changes in the operational environment (multi-domain) and the movements of the adversary. Operating in this manner ensures that the transition from peacetime to crisis or conflict is managed as effectively as possible.

The complexity and speed at which the operational situation changes, coupled with the impact of multi-domain capabilities (such as electronic warfare and Intelligence) have driven an ever-increasing need for real-time information processing and data analysis. This has inevitably led to a greater reliance on automation (HOTL) to help expedite the analytical process to ensure that opportunities are not missed.

As previously discussed, in the multi-domain C2 process, the use of tools such as Big Data and AI are considered especially vital due to their ability to analyse and prioritize according to algorithms without human involvement in the process. Systems that can perform multiple simulations and decide the best courses of action are essential as complex scenarios can quickly saturate human analysis capabilities. This can cause coordination and synchronization to be more difficult and responses may not be fast enough to fully exploit advantages. AI reduces information overload, improves situational awareness and supports the decision-making process. All this shortens the C2 cycle.

The targeting cycle is a good example. The entire process from track detection, analysis, prioritization (tasking and re-tasking) right through to re-attack, can be automated based on a number of pre-programmed parameters that reduce the timescales involved.

Presently, AI cannot completely replace the requirement to have human input in the decision-making process of a multi-domain C2 network. In modern warfare, intuition and common sense are always necessary and good judgment is fundamental. The HITL applies judgement, knowledge, and reason to new situations that do not resemble previous experiences. It is in these scenarios that AI is truly challenged, because it is not easy for AI to analyse situations and environments that it has not encountered before. To mitigate this problem, a form of ML programme is required that can adapt to changes. However, once the decision to take military action has been made, many additional factors must be considered that can heavily influence the use of force. More intuitive, ‘softer’ factors such as legal and ethical considerations are far harder to program. All of these aspects must be considered in a comprehensive C2 system to facilitate timely decision making; both in the planning and execution of an operation.

Multi-domain C2 is of particular importance for Air forces. The key Air Power attributes of height, speed, and reach require a high degree of pan-domain mission prioritization and synchronization. In addition, Air Power's strong dependence on technology makes it especially vulnerable to attacks in the domains of Cyberspace and Space. Our requirement to use Space for a wide range of activities (communications between aircraft and C2 systems, accuracy and guidance of our weaponry) will inevitably increase and become more critical in the future due to technological advancements in next-generation aircraft, unmanned aerial vehicles, and for real-time intelligence information.

For these reasons, it is necessary that all activities in all domains be synchronized in the C2 process to ensure that competing requirements are managed as effectively as possible. In addition, it must be done dynamically, adapting to the changes that occur as the situation evolves during operations.

The requirement for rapid data analysis requires us to maintain well-trained, experienced operators during peacetime who can be relied upon during crisis or conflict to calculate risks quickly and provide accurate advice and recommendations to inform a Commander's decision-making.

The proper distribution and dissemination of information to those who need it is also essential so that action can be prioritized and reaction times shortened as much as possible, which is vital for Air activity.

In NATO, any new C2 system must coexist with legacy systems as all allies may not update their technologies at the same rate. It is important that such systems are able to interoperate with one another and that the operators using legacy systems can connect and work with those using newer ones (and vice-versa). A degree of standardization at the developmental stage is essential, so that the Alliance can continue to work together. Only in this way can we preserve unity of command. However, we must also ensure that any move towards a less-federated C2 system does not come at the cost of resilience or integrity.

Conclusion

New geopolitical scenarios and the development of technology in multiple fields make it necessary to adapt the process of planning and executing military operations. We will continue to face challenges that inevitably appear with little warning, particularly within the aerospace domain.

Technological advancements are driving the development of new weapons systems in all domains (unmanned vehicles on Land, Sea, and Air with automatic targeting; hypersonic and radar directed weapons; lasers) and new operating procedures must be developed at a similar pace. These new weapons systems and the new possibilities they offer require modern C2 systems that are capable of harmonizing and working in a synchronized manner across domains. For these reasons it is necessary to work more on the concept 'Joint All Domain C2'. This means that all personnel who operate as part of a C2 system, from the operators (employing AI or Big Data) to the commanders, have to be trained and able to harness all the tools available (HITL, HOTL and HOOTL) in order to refine the decision-making process.

NATO must continue to adapt and modernize to consistently analyse current and future risks in peacetime and be able to respond dynamically to protect allied nations.

To this end, NATO is promoting a culture of continuous improvement among all allied countries regarding weapon systems, C2 means and collective learning. Of course, not everyone can evolve at the same rate; therefore we must use legacy systems together with the most advanced ones and make them truly interoperable.

Lieutenant General Fernando De La Cruz Caravaca (SP Air Force) is the Commander of NATO's Combined Air Operation Centre at Torrejón Air Base, Spain. He holds a Master's Degree in Security and Defence from Complutense University in Madrid, Spain. He is a graduate of the Spanish National Defence War College and the NATO Defence College.

© solarseven/Shutterstock.com

1X

Is Human-On-the-Loop the Best Answer for Rapid Relevant Responses (R^3)?

By Dr Michael Cowen,
Capt (ret.) Rick Williams, US Navy, and
Brig Gen (ret.) Doug Cherry, US Army
Monterey Technologies, Incorporated

Introduction

In this paper, we address three high-level questions that we recognize do not have clear answers as yet. Is a Human-On-the-Loop (HOTL) capability, giving user control only over autonomy planning, better at delivering Rapid Relevant Responses (R^3) than Human-In-the-Loop (HITL), where the user has complete control to start or stop the automation? Can we adapt current HITL Command & Control (C2) architectures using variable autonomy to address compressed cycle times and more demanding time constraints in the hypersonic operational environment? And do we dare risk Human-Out-Of-the-Loop (HOOTL) weapon systems and the potential for control-induced errors caused by brittle automation that can lead to cascade failures? At issue is how to evolve these high-level questions toward operational answers.

Warfighters for many years, and from many warfighting domains, have demanded more capability and functionality in the weapons and systems they are given. 'We need it to do more' has been the common theme, regardless of Allied Command or branch of military. We have now reached the stage of technology development where engineering teams can build more capability and functionality into weapons and systems than our warfighters can extract, given the current state of user interface design, because the human operator typically is a complete afterthought for systems design teams. As technology continues to move forward in leaps and bounds, we must shift the focus from designing more functionality into weapons and systems to developing the next generation of C2 architectures to allow our warfighters to extract 100 % of the functionality built into these systems while reducing required training time. The focus of this paper is major weapons and C2 systems and the challenge of hypersonics. In the future, the lessons learned can extend across echelons from strategic/operational levels to tactical platforms and individual warfighters.

The purpose of C2 is to enable the effective transfer of information between and among systems and operational users to gain situational awareness, make decisions, and execute appropriate courses of action. There are several methods available to designers, acquisition professionals, weapons developers, and warfighters. HITL methods develop tools to facilitate the effectiveness and ease of knowledge management, information foraging and exchange, collaboration, and decision-making in the networked command environment. It is essential that C2 architectures consider how to effectively integrate operational users with information technologies and networks, particularly as weapon velocities approach hypersonic. The tasks that must be accomplished by command decision-makers are time-critical with life-or-death outcomes. In this context, human performance must be optimized to deliver R^3, but no amount of training can compensate for poor human systems integration and confusing user displays that obfuscate automation status and human control. HITL is mandatory during test and evaluation, training, and early-stage fielding into operational theatres. A progression from HITL may require a precautionary phase of HOTL as a step toward higher levels of autonomy to HOOTL. Our discussion focuses mainly on performance improvement of HITL routines which may have implications for the human in/on/out of the loop progression.

Technical Approach

Graceful degradation is an automation supervisory control technique that we propose to explore. Automation features are needed that sense, analyze, and react to platform/vehicle/weapon environmental conditions and equipment status and can adjust R^3 subsystems to maintain normal operations. Problems occur in the human-system supervisory loop if the adaptations suddenly cross a tolerance threshold wherein the system rapidly fails. Automation that can rapidly fail is referred to as 'brittle' because it breaks suddenly and without warning. Graceful degradation is needed whereby the human supervisors are informed and aware that automated features are compensating for performance deviations. Users then must be trained to view and interpret this information.

For example, automation for an Unmanned Surface Vehicle (USV) may increase boat engine thrust and power to maintain R^3 payload launch position to deal with strong currents or a propeller fouled by seaweed. Plans for task process contingencies can be based upon the availability of information (e.g., can inspect in and around the USV with no blind spots) or known information deficiencies (e.g., can measure ocean current and resistance, but cannot inspect for a fouled propeller). While the automation rules may require that engine RPMs above a certain value require instant corrections to maintain speed/schedule, the automation must also be able to immediately inform the user about the rate of change and direction, beyond the reported fault information from the automated correction. The operator must be in the information loop as automation makes adjustments to maintain operations. This example is relevant and critical to modelling how experienced warfighters would respond as cycle times approach zero when launching, or defending against, hypersonic weapons. A design approach to mitigate the effects of brittle automation should consider graceful degradation that clearly warns the operator of deviation while reducing automation, to prevent automated courses of action in degraded modes that could lead to cascade or catastrophic system failures. Employment of R^3 HITL contingencies should be based upon the availability of information or known information deficiencies.

Another supervisory control issue is automation-induced complacency. Automation complacency (aka, automation bias) is the condition that occurs when users tend to trust the automation results and disregard other possible contradictory information. Factors that contribute to complacency include long periods of stable operations with few critical decisions, monotony, fatigue, and boredom. Mitigation strategies can include tasks and activities designed to keep operators alert, diligent, and vigilant. Simulation of events and recurring practice and activities with critical events can also reduce negative issues related to complacency. Endsley's model[1] of autonomy oversight recognizes the 'decision-biasing effect' of operator dependence on automated decision aids. Human operators tend to supervise automated systems using approaches that require the least cognitive effort when seeking and sharing process details, believing that automation has superior analytical ability. R^3 architectures should consider decision process designs that grant active human 'management by consent' versus reactive 'management by exception' to mitigate automation bias by requiring the human operator to remain actively engaged, except in delta near-zero situations. The effects of automation bias will be greatly reduced by explicitly displaying decision elements/steps, and then compelling the user to engage in the decision process with critiquing, what-if, and contingency planning paradigms.

When mitigating the effects of automation bias, the decision process to support 'management by consent' or 'management by exception' must also be able to manage cognitive biases of human information processing, especially under conditions of high workload.[2] These biases have been found to be the underlying cause for most errors in human judgement and have been extensively studied.[3] HITL architectures must address potential human judgement errors in the supervision of R^3 tasks and workflows, most notably confirmation bias, availability bias, and illusory correlations. As with automation bias, the best way to reduce judgement bias is to explicitly (and in an operationally relevant manner) display layers of information and data that both support the decision process and engage the user.

Task-Centred Design (TCD)

HITL R^3 architectures should support warfighter tasks. TCD organizes system information and controls in a human activity-centric manner such that normal workflows are efficient and task products can be easily created. In a task-centred design, information is 'brought to the task' versus requiring the end-user to collect, gather, and synergize information from separate sources TCD for R^3 operations will involve the trade-off of function allocations between human and system for doing task steps and accomplishing goals.

When function allocation design decisions are made, User Interface (UI) constructs can be created to deliver capability as cycle time approaches zero. This can include shared system-user task states and awareness of past, current, and planned tasks explicitly listed. A UI construct to foster task-centred performance can include the explicit display of tasks which are triggered based upon mission objectives. For example, Osga[4] developed a task management display which depicted completed, current, and emerging tasks for a dynamic ship defence combat information team operating environment. The display represented task states in the form of icons associated with ship defence and related battlegroup reports. The reduction of cognitive workload related to the analysis of raw data, finding tasks, and creating task products allowed the operators to shift cognitive functions towards higher-level mission supervision and away from continuous information search and filtering sub-tasks.

HITL Modelling

R^3 requires the exploration and analysis of the degrees of freedom, constraints, and consequences associated with developing automated sensors, platforms, and weapons systems, modelling the advantages and disadvantages of HITL, HOTL, and even HOOTL. This modelling needs to be an essential part of the thoughtful development and testing of sensors and weapons systems. HITL, HOTL, and HOOTL system development must consider the capabilities of expert systems, Artificial Intelligence (AI), and Machine Learning (ML) at all levels of embedded logic and include a careful review of all components, assemblies, subsystems, systems, and systems-of-systems.

We propose a ML R^3 testbed to evaluate application ideas and tools to improve response accuracy and scheduling, creating algorithms to mine what strike teams think about when considering options. The testbed will evaluate what decision-making heuristics should be considered to do response planning in tactical environments and to provide intelligent strike assistance to any response team. HITL can be done using Interactive Learning (IL) methods. IL is an artificial intelligence ML approach with a human in the machine interactive loop, where observations of user interactions are recorded to provide guidance for the next ML iteration and improve machine accuracy. We propose a ML active learning approach, which asks Subject Matter Experts (SMEs) to label only the most important strike planning data via pool-based active learning, identifying cognitive patterns to train a strike planning aid. Using interactive learning methods, we can evaluate computer-generated strike plans given an R^3 objective using multiple fix sources to model and accurately estimate red threat location.

With this methodology, we can discover algorithms that capture what warfighters think about when deploying R^3 to better understand what decision-making heuristics should be considered to facilitate tactical planning in evolving battlespace environments. Specifically, we will conduct limited objective experiments using IL methods to cognitively model how SMEs evaluate automated strike plans to discover core tactical and operational planning heuristics as the basis for smart algorithms to increase speed and efficiency of the mission planning and execution process. This currently involves a significant amount of error analysis that is done in the head of the warfighter. Here, we can generate and test algorithms to capture what the warfighter thinks about when figuring out the best course of action. The HITL model can then be refined to get a clearer idea of what decision-making heuristics the warfighter should be considering to achieve better strike options. Via iterative design and testing, we can express and build a reliable machine learning paradigm by arranging the heuristics and algorithms into an operational view, which could be applied to other strike planning domains to create AI requirements for more effective UIs to support mission strike teams.

Using IL methods, we will evaluate automated kill chains for R^3 objectives. Algorithms must integrate across multiple perspectives: risk, probability, uncertainty, complexity, consequences, and accountability. International boundaries, threat assessment, blue platform/weapon status, and human supervisor experience level must all be part of the equation. We will also model the challenges of determining threat location in GPS-denied, Radio Frequency (RF), Emissions Controlled (EMCON), night and cloud-covered scenarios. The IL modelling will begin with a series of experimental trials where the SME will choose the better of two displayed automated strike options, followed by the display of more machine-suggested options and so on. SME's comments will be captured, noting reasons for selecting/not selecting a particular option. The testbed will collect choice data and capture the n-dimensional state of the scenario including HITL role, blue capabilities, threats, fix location source availability, and display layout.

Conclusion

Increasing levels of automation and AI bring the promise of enhanced weapons effectiveness, but also bring risks that may lead to lethal consequences. We propose a variable autonomy method to adapt C2 HITL architectures to address compressed cycle times and more demanding workloads in the R^3 operational environment. This methodology will offer control solutions to mitigate the risks associated with HOOTL weapon system options where machine errors and brittle automation can lead to cascading failures. A C2 architecture approach to address the effects of brittle automation should consider design strategies that model R^3 automation to make the human operator more aware of deviations from the strike plan, changes to the weapon system state, and pending automated course of actions. This requires in-depth human factors analysis of how weapon system autonomy progresses from HITL to HOTL to HOOTL and how automation supervisors reassert control and retain decision-making while minimizing response delays. The actions, reactions, and consequences associated with R^3 automated systems are and will be, in the final analysis, the responsibility of the human warfighters and Joint Force Commanders who ultimately will employ these current and future capabilities. This requires modelling of how the most experienced warfighters would react to deviations and high consequence/low-frequency scenarios, particularly as cycle times approach zero to launch and monitor, or defend against, hypersonic weapons.

Dr Michael B. Cowen serves as a Senior Human Systems Integration Professional of Monterey Technologies, Inc. and Director of Human Factors Engineering. He has a PhD in Cognitive Psychology, a MS in Industrial/Organizational Psychology and a BA in Experimental Psychology. Dr Cowen is a former Naval Information Warfare Center researcher working over 37 years at the Point Loma campus as a Human Factors Psychologist.

Captain (ret.) Rick Williams (US Navy) is MTI's Chief Technologist. His 45 years' experience in public and private sectors includes 21 years of continuous sea duty as a Surface Warfare Officer, Submarine Warfare Officer, two afloat commands, and US Third Fleet N6/J6/J9. He is a Project Management Professional, New Product Development Professional, and Defense Acquisition Professional.

Brigadier General (ret.) Doug Cherry (US Army) is MTI's Chief Executive Officer. He has 37 years' experience in the Army before joining MTI. He has commanded from the Company to the Division level. He served in the operational Army, including overseas, as well as the Institutional Army, including Pentagon assignments. In the Institutional Army he served as a force developer with experiences ranging from new material requirements to manpower and organizational design.

Endnotes

1. Endsley, Mica R., 'From Here to Autonomy: Lessons Learned from Human-Automation Research', Human Factors, no. 59 (2017): p. 5–27.
2. Kahneman, D., Thinking, Fast and Slow, New York: Farrar, Straus, and Giroux, 2011.
3. Lewis, M., The Undoing Project, New York: W. W. Norton & Company, 2016.
4. Osga, G., Van Orden, K., Campbell, N., Kellmeyer, D., & Lulu, D., Design and Evaluation of Warfighter Task Support Methods in a Multi-Modal Watchstation, Space & Naval Warfare Center San Diego Tech Report 1874, 2002.

© Andrea Danti/Shutterstock.com

Technology and Connectivity

X

An Essential Bond for a Modern Air Force

By Maj Ferdinando Pagano, IT Air Force
Italian Air Force Staff

'Any Air Force which does not keep its doctrine ahead of its equipment, and its vision far into the future, can only delude the nation into a false sense of security.'

General Henry H. Arnold[1]

Introduction

Air and Space Power (A&SP) are intrinsically linked with technology and connectivity, in fact, they are two sides of the same coin. To fully understand the complexity of modern A&SP, it is paramount to consider the specificities of the aerospace environment as well as the implications of technological evolution within the Air domain.

Today, modern Air Forces are required to operate in the third dimension at supersonic speeds, guarantee the persistence of the Air power in operations, even when operating far from home, and support Land and Sea components, including the projection of forces. All these elements cannot be satisfied without the extensive use of advanced and innovative technologies.

Since its beginning, the aviation world has been strongly influenced by the evolution of technology. Over the years, the application of and experimentation with emerging technologies have been applied to A&SP and their use has gradually increased as an essential requirement for any complex military operation involving A&SP.

Technological innovation today has seen a 'rate of change' never before experienced. This is due, at least in part, to the extensive use of new technologies which have expanded the upper limit of the aerospace dimension from 20 km, which historically was the customary boundary regarding commercial and military flights, to 100 km, the conventional border between the aeronautical (or Earth's atmosphere) and Space environments (or Outer Space) known as the 'Karman Line'.

Technological advancements will soon produce both suborbital carriers and hypersonic vehicles that operate with greatly increased range, such as more focussed cyber-attacks, swarms of drones, and new systems that exploit the advantages of robotics and artificial intelligence. The latter, in particular, will allow the automation of highly complex processes, manage the storage of huge amounts of data and process that data via Edge Computing[2], with the aim of maximizing information collection in the area of operations (information superiority) and enabling fast decision-making models (decision superiority). An essential element of the previously mentioned decision-making superiority is interconnectivity or digital connectivity. It can be defined as the technology that will allow all the different systems present in the operational environment (in NATO's five operational domains) to be connected and able to exchange information in near-real time for the benefit of key decision-makers (from the commanders in the field, up thru the political authority).

From Analogue to Digital Connectivity

The exploitation of the radio sector of the electromagnetic spectrum, via wireless technology, which initially aimed to improve communications in military operations, has undergone a progressive and radical transformation thanks to applications based on Internet Protocols (IP). These applications have allowed for the transfer and sharing, in real-time, of information coming from different channels.

Today, in the digital era, which includes the Internet of Things[3] (IoT), the ability to interconnect various devices has become a consolidated and essential requirement for the collection, exchange, distribution, and storage of information (so-called Big Data[4]). The Digital Connectivity, defined as the ability to connect sensors in a 'system-of-systems'[5], is the main enabler of decision superiority.

Achieving Air superiority, however, is a more complex endeavour than a 'simple, combination of systems and Digital Connectivity will soon become the decisive factor in the conduct of Multi-Domain[6] Operations (MDO[7]). In order to ensure continuous information sharing between commanders and operators in the field, interconnected systems will be required to be highly resilient and 'intelligent.' This will ensure a speed of command and control that will transform the advantage of information (or Big Data) into real decision superiority over the adversary. Interconnectivity will create a shared picture of the theatre of operations capable of connecting the right sensor to the right effector at the right time (sensor to decision-maker to shooter) to create complex dilemmas for the adversary.

Paraphrasing General Denis Mercier[8] (FR), it can be assumed that the keyword for the Future Combat Air System (FCAS) is indeed 'system'. In fact, it will not be a manned aircraft or a drone, but a system of systems integrating, within a cloud, sensors and effectors of various types and different generations. And, the backbone of this system will be a Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance core.

The Joint Nature of Air Power and the Merging of New Domains

Since the recognition of Air as a separate operational domain, Air Power has been intrinsically multi-domain by nature. Historically, armies and navies expressed their power by acting in the domains of Land and Sea, respectively. Only with the advent of the aircraft, did military operations become truly joint, and today no operation can occur without the support of aerospace capabilities.

In this vein, for a modern Air Force to keep its 'joint-by-design' feature and effectiveness (which differentiates the Air Force from other armed forces), it is necessary to broaden the joint approach to the emerging domains, such as Cyberspace and Space.

As a matter of fact, Air, Space, and Cyberspace operations have developed an interdependent relationship that grows day by day. Space and Cyberspace resources (i.e., satellites, antennas, and waves transmission) are, in fact, inseparable from the third dimension, and similarly, Air operations use computer networks and Space assets regularly. As indicated by General Mercier, due to this interdependence to fight in the Air and in Cyberspace, it was mandatory for the Air Force to include the nature of this new strategic environment. He recognized the ability of Space and Cyberspace operations to improve and support 'conventional' operations through the intensive use of new technologies which push for greater and greater interconnection every day. In fact, to allow Air Power to use the full spectrum of modern technologies, it is critical to recognize that connectivity has a leading role.

Multi-Domain Operations and Connectivity

As previously mentioned, the power expressed by the Air Force has always been extended to the other physical domains (Land and Sea) and, in the future, is going to be more and more interconnected to the emerging ones, namely Space and Cyberspace. This requires an evaluation of the threat coming from new and emerging technologies, which has evolved with all available means, rapidly, often at low cost, and from not well-defined sources to deny the strategic advantage gained by AP.

Consequently, a requirement for Air forces is to develop the ability to coordinate, at national and multinational levels, the delivery of synchronized effects in multiple domains in sequence or, preferably, simultaneously.

However, this involves a significant conceptual evolution, as it moves from the current joint and inter-agency construct (already complex and articulated) to a multi-domain approach which, with the integration of Cyberspace and Space, allows for the conduct of MDO or, in the most recent terminology, Joint All-Domain Operations (JADO).

In this context, the goal of a modern Air force will be to develop an ad hoc info-structure, based on Internet Protocol, and to use a combat cloud capable of connecting all sensors, effectors, and command and control nodes in real-time. Contextually, it will use the emerging technologies (e.g. artificial intelligence) associated with, and in support of, the human component.[9]

Emerging Technologies and Connectivity

The use of emerging technologies[10] in the military sector, as well as in all civil and economic sectors, is certainly aimed at pursuing a concrete competitive advantage.

Intelligent and more autonomous systems capable of transferring and processing enormous amounts of information are supplanting and overcoming some typically human capabilities.

To date, such autonomous or semi-autonomous systems have been limited, requiring rigid operating rules and direct human control. The use of artificial intelligence will allow new systems to enable increasingly sophisticated decisions (through ad hoc algorithms) and will create a new complex concept of the 'man-machine' team. Future intelligent systems will provide, from the strategic to the tactical level, rapid analysis, advice and courses of action which will enable an increased effectiveness of the Observe, Orient, Decide and Act (OODA) cycle and therefore allow for more innovative strategies.

In order to get the advantage offered by these technologies, it will be essential to ensure the interconnection between domains, and between sensors operating in or through them. By carrying out functions of collecting, processing, and exchanging information, they will fulfil the prerequisite to achieve Decision Superiority.

Connectivity: The Centre of Gravity for Future Aerospace Systems

Therefore, Digital Connectivity (or Native Digital Connectivity), represents the centre of gravity of future aerospace systems. Starting from Clausewitz's definition of 'the hub of all power and movement, on which everything depends', it is possible to use the metaphor of the human body to illustrate the analysis of connectivity as the centre of gravity for modern and future Air forces. The human body would not function without a heart, but today's technology can keep a human body alive by using an alternative energy source. The joints provide physical strength and movement but complement the 'human body system' and are not its centre of gravity. The brain, instead, represents a source of power. It can provide the physical body the will to act and then the ability to do so. Still, without blood flow and oxygen (connectivity), the brain would stop functioning and with it the control centre of the entire body. Implementing the connectivity principle in the development of future aerospace capabilities is therefore crucial. The 'native' interconnection will allow the new generation and advanced systems to act as a 'single entity', within a 'system-of-systems', and be able to realize the integration of all relevant information. This will concretely improve the Commanders' decision superiority, at all levels (strategic, operational, and tactical), as well as the ability to anticipate and rapidly respond to new emerging threats coming from all domains of operations.

Therefore, capability development will have to evolve in the direction of 'Native Digital Connectivity'. This will transform today's information technology into a more competitive advantage of tomorrow. In that venue, collaboration with industries and academia is strongly envisaged, as well as the enforcement of the current paradigms of cyber-resilient-by-design and cyber-resistant-by-design. In short, any new future aerospace capabilities will have to be designed and developed considering Native Digital Connectivity and Cyber Security as intrinsic requirements.

Conclusions

The future of technology and programs are clearly and unambiguously moving towards increased system integration and connectivity, where each platform is no longer a stand-alone system but part of a distributed and connected intelligence. Therefore, technological development represents a challenge, but also an opportunity that cannot be missed. It is a train that does not stop and does not wait, and to which all Air forces and members of the aerospace industry must remain connected, otherwise, they will face future irrelevance. Recalling the words of General Giulio Dohuet: 'Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.'[11]

Major Ferdinando Pagano (IT Air Force) is assigned to the Italian Air Staff in the General Planning and Transformation Office as a CIS and Cyber Officer.

Endnotes

1. General of the United States Army Air Force (USAAF) in the Second World War, theorist of strategic bombing and the independence of the air component from the Army and Navy.
2. Distributed computing paradigm that brings computation and data storage closer to the location where it is needed in order to improve response times and save bandwidth.
3. Extension of the Internet to the world of real objects and places.
4. Extensive data collection in terms of volume, speed and variety that requires dedicated analytical technologies and methods for the extraction of value or knowledge.
5. Complex system that offers more functionality and performance than the simple sum of the subsystems. In the aerospace domain, it implies the ability to connect in a single 'information cloud' piloted elements with other unmanned or even autonomous elements. This principle can be further extended to the whole operational environment, in which all the different 'information clouds' are interconnected.
6. Air, Land, Sea, Cyberspace and Space.
7. MDO: as reported by JAPCC at https://www.japcc.org/conference-proceedings-2019-theme-1/, Multi-Domain Operations (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.
8. 'Les opérations aériennes et le cyber: de l'analogie à la synergie', 2015.
9. To ensure compliance with law and ethics principles.
10. Including Emerging Disruptive Technology (EDT): Big Data, Artificial Intelligence (AI), Autonomy, Space, Hypersonic, Quantum, Biotechnology.
11. General Giulio Douhet, 'The Command of the Air', 1921.

© Timofeev Vladimir/Shutterstock.com

Multi-Domain Combat Cloud

XI

A Vision for the Future Battlefield

By Col (ret.) Hubert Saur, GE Air Force
Airbus

Introduction

***'… lack of information sharing impedes operational effectiveness. Information sharing restrictions and national caveats limit interoperability solutions and reduce operational effectiveness across the domains.'*[1]**

This is one key finding of the Joint Air Power Strategy – Interoperability Study from January 2020. To overcome this shortfall, it requires a far higher level of automation and integration throughout the mission cycle.

The operational environment continues to change at high speed. Future military operations call for collaborative, more efficient, digitized, secure and cyber-resilient battlespace across Land, Air, Maritime, and Space domains.

Intelligence-driven operations and effects-based planning have been two principles proven valid for decades. Every operation starts with the assessment of an evolving crisis. This is the phase where we observe and orient. During this initial process, we are already gathering tremendous amounts of data, analysing, assessing and transforming them into information to be disseminated among the key actors, striving for information superiority. Considering the fact that seconds or even milliseconds will make the decisive difference between survival and destruction in a contested military environment, Multi-Domain Superiority will only be achieved through complete situational awareness based on data and advanced analytics to assist fast and more accurate decision-making. Therefore, future warfighting will require a far higher degree of processing, automation and integration throughout the mission cycle. To tackle these challenges, this paper argues on behalf of a Multi-Domain Combat Cloud (MDCC) solution to enable forces to 'Be Informed as One and Act as One'.

What Is a Multi-Domain Combat Cloud, and What Will the Operational Benefit Be?

A 'Combat Cloud' is a connectivity of nodes, a dot-based elaboration of a cloud environment. This paper is proposing far more than what is typically seen as a network-attached cloud environment for the storage and processing of valuable data. What is required is a concept which strives for connecting manned and unmanned platforms, human-operated and human-controlled, but Artificial Intelligence (AI) supported systems.

NATO forces need to accelerate the operational tempo when completing Observe Orient Decide Act (OODA) loops better and faster than the opponent to take control of the situation. To overcome an opponent whose forces constitute a complex adaptive system, agility is key.

The objective is to get inside an opponent's OODA loop, forcing a response to a situation that is no longer relevant.

A MDCC will speed up the OODA loop by providing common situational awareness through the instantaneous capturing, sharing, merging and processing of massive amounts of data from all connected manned and unmanned assets, by supplying predictive intelligence and assisted decision making, by allowing mission planning and re-planning: The enabler for distributed decision making and collaborative combat.

The envisioned approach is about merging data from various sources in a trusted way and turning that data into actionable information thanks to the latest analytical and learning technologies. Being able to share right information, at the right time in the right place will provide information superiority.

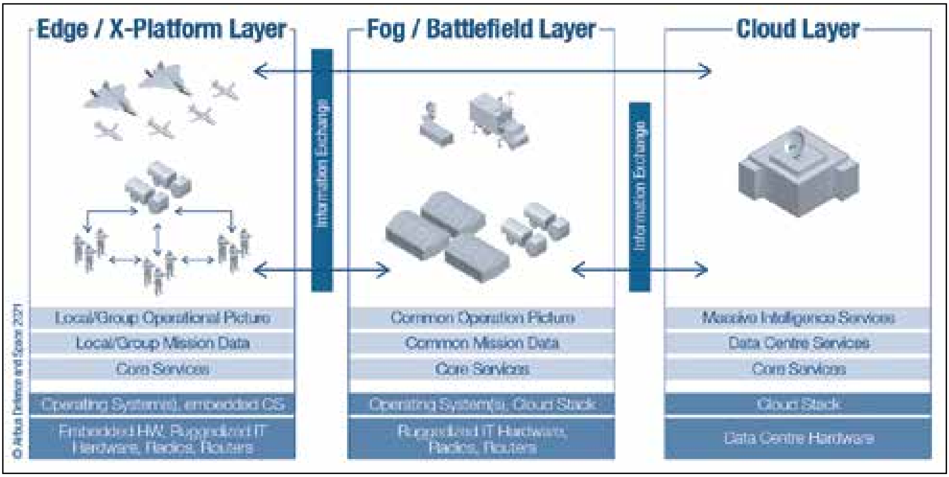


Figure 1: *Cloud, Fog, and Edge Layers.*

Informed as One – Seamless Exchange of Validated Information as Key Element in the MDCC

The MDCC shall be the enabler for joint all-domain operations at each command level, i.e. strategic, operational, and tactical. The same technical services and algorithms will be running on cloud servers in headquarters, in containers in forward operating bases, as well as on fighter aircraft, tanks, or ships. The aim is to achieve a seamless exchange of validated information at different layers leading to information superiority.

The Cloud Layer contains all systems which deal with large amounts of data. In general, these systems are only a few and the location of the systems is not relevant in the context of the operation.

For future MDCC add-ons we can expect a data-driven collaboration across assets and domains, including for example:

- high-level automation of data exchanges;
- predictive analytics and scenario calculation;
- wide area connectivity management;
- faster Planning Cycle;
- increased post-mission awareness.

The Fog Layer deals with a lesser amount of data linking the Cloud and Edge. It is envisaged to be a deployable or even mobile data node with high computing capability but compared to the cloud layer with limited data storage capacity. In general, these systems are only a few to many and the location of the systems is relevant in the context of the operation. In current operations these could be an AWACS or a smart MRTT.

For future MDCC add-ons we can expect smarter information sharing and decentralized autonomous combat Command and Control (C2), including:

- higher flexibility and dynamic reactivity on real-time changes;
- increased Situational Awareness by distributed collaborative sensors;
- reallocate dynamically C2 roles between assets and nodes.

The Edge Layer contains systems which predominantly contain effectors and/or sensors. In general, these systems provide the data and lower-level information which are consumed by systems in the Fog- and Cloud Layer in order to generate higher-level information or intelligence.

For future MDCC add-ons we can expect a higher level of collaboration of manned and unmanned assets, including for example:

- C2 of unmanned assets;
- high-level automation of flight management;
- continuous shared information;
- continuous re-planning;
- common operational picture.

The Core – Multi-Domain Combat Cloud Architecture

Throughout the complete mission, cycle data are collected from various sensors across all domains, which need to be transferred into actionable information provided to all actors and nodes through a common or shared information space. All actors need to work with and on a Common Relevant Operational Picture regardless of their task. This is a prerequisite for synchronized collaboration beyond the boundaries of component commands and domains.

A MDCC will need a modular, scalable and flexible architecture to meet current and future unknown threats. Using standardized interfaces, the communications services will interconnect the sensor, effector and C2 nodes belonging to the various assets to allow real-time and/or near-real-time resilient secured linking. Such communication services will consist of communication networks, transmission systems, relay stations, tributary stations, and terminal equipment capable to form an integrated whole.

Turning the connected assets into actionable sensing, effecting, and C2 nodes will require interoperable information systems defined as 'Core Services'. This allows disaggregating of operational functions into applications and services and aggregating massive sets of data on a common cloud platform. Such information systems are integrated sets of components for collecting, storing, processing, and distributing data to deliver validated information.

Ensuring that all actionable nodes can collaborate across the C2 process will require the background capabilities defined as technical services in support of all mission types and operational capabilities. Such technical services will be hosted on multiple physical platforms across Air, Land, Sea, and Space to ensure resilience. Within a given platform, each actionable node will be a requester and a provider for technical services. Load balancing between receiving and providing data and information will be dynamically managed to ensure optimum performance considering the given constraints.

The technical services requirements will be derived from the operational needs expressed by the collection of User Facing Capabilities. Technical services will, according to the Consultation, Command and Control (C3) NATO Taxonomy,[2] include the Community of Interest Specific Services and Enabling ones.

Act as One – the Application and Information Layer

Human-Machine Collaboration will be key to Human Facing Applications so that humans can focus on supervising and deciding in constrained environments rather than processing and tasking. Such meaningful human control is commonly referred to as human in or on the loop.

Within the overall system of systems of actionable nodes, multiple effect paths will be running concurrently. In light of such complexity, AI will be required to orchestrate the different actionable nodes and to manage massive data which will empower the C2 process.

Delivering information and digital products to a network of connected platforms also provides opportunities for cyber-attacks. End-to-end robust cybersecurity will allow protection and timely response to attacks or threats to prevent the tampering of infrastructure and/or the 'injection' of fake data and/or malware.

Service structuring of MDCC architecture enables an efficient, effective, and relevant supply of validated information with the same information but automatically optimized for each user. Supported by the application, the user decides on the purpose of the information provided in a cognitive manner. Orchestrating the different actionable nodes and managing the massive amount of data generated during the mission cycle requires AI and Machine Learning (ML). With advanced analytics and AI the Observe and Orient phases of the OODA Loop will benefit through quality and time thus reducing the workload of the human beings allowing them to focus on the Decide and Act phase. AI and Human-Machine Collaboration will contribute to information and decision superiority ensuring meaningful control throughout the mission cycle.

Conclusions

Thanks to long-lasting experience and projects in the defence area, a MDCC is/will be compliant with current and evolving C3 NATO

Taxonomy and thus provides an essential basis for synchronization and interoperability.

The main advantage of such MDCC architecture is the modularity and scalability for the development of applications. It allows creating new services, orchestrating them differently and deploying them in a flexible way. Agility and flexibility within the delegation of C2 for example, within the context of Alliance Future Surveillance and Command System rests on service structuring.

The usage of open standards and well-defined service 'Application Programming Interfaces' allows building interoperable applications for a multi-vendor environment such as the Multi-Domain battlespace. Depending on the technical state of play, different national operational applications can be safely integrated into such Combat Cloud architecture. This allows for synchronization as a prerequisite to act as one.

Colonel (ret.) Hubert Saur (GE Air Force) joined the German Luftwaffe in 1982 and retired in 2017. Within his military career, he achieved more than 1,500 flying hours on combat aircraft, mainly Tornado IDS and ECR. He holds a Master's Degree in National Security Strategy from the National Defense University, Washington DC, USA.

Endnotes

1. NATO Supreme Allied Commander Transformation (SACT), NATO's Joint Air Power Strategy (JAPS) Interoperability Study, 15 Jan. 2020, p. 7.
2. NATO, Supreme Allied Commander Transformation (SACT): C3 Taxonomy Baseline 4.0. ACT /CAPDEV/REQ/TT-2895/Ser: NU: 0716, Norfolk, 10 Jun. 2020.

© K_E_N/Shutterstock.com

NATO Command and Control Resilience in Contested Environments

XII

By Mr Owen J. Daniels and Ms Clementine G. Starling

Institute for Defense Analyses/Scowcroft Center for Strategy and Security, Atlantic Council

As competitors aim to disrupt communication and coordination among NATO forces, the Alliance's ability to maintain Command and Control (C2) will be paramount. NATO must adapt to improve its C2 resiliency and consider new concepts for operating in contested environments, especially as Allies explore technological and systematic changes to their C2 structures. The United States is adapting its C2 structure with concepts like Joint All Domain Command and Control (JADC2) and NATO Allies should weigh similar approaches to bolster combat effectiveness, ensure integration, and maintain interoperability in degraded C2 environments. This article presents ongoing and future C2 challenges for NATO and possible approaches for improving C2 resiliency.

NATO's C2 Challenge in Contested Environments

Russia poses the most likely contested environment dilemma for NATO. Russian Anti-Access/Area Denial (A2/AD) tactics could limit NATO's ability to establish strategic advantage at its doorstep even before a conflict, disrupting NATO efforts when 'fait accompli' scenarios erupt.[1, 2] A2/AD prevents opponents from accessing key areas and denies manoeuvre, allowing adversaries temporal advantages to achieve effects before the warfighting space can be contested. Anti-access could prevent NATO from projecting power into the battlespace, enabling adversaries to favourably change facts on the ground. The S-400, Bastion anti-ship system, and Iskander ballistic missile comprise the core of Russia's A2/AD suite and work in concert as deterrents against potential NATO responses to aggression.[3] Russia demonstrates its denial capabilities in the Arctic, Baltic, and Black Sea regions; no-go 'bubbles', like the Kaliningrad exclave, aim to deter NATO action by signalling impregnability.[4]

NATO's C2 nodes and infrastructure in kinetic and non-kinetic domains, critical to any contingency fight, will likely be among the first targets in a contested environment. Operational C2 impacts battle management and forward force projection – disrupting it holds appeal for adversaries less capable than NATO. C2 denial could complicate NATO's vision for supplying, sustaining, and reinforcing forward forces, like enhanced Forward Presence battlegroups in the Baltics, and disrupt NATO's overall force projection ability and collective response. In manoeuvre warfare, A2/AD disrupts information flows and command between sensors and shooters. With inadequate preparation, tactical forces could struggle to contribute to combined effects, hampering the strength of the force. Further, NATO's air power is vulnerable to electronic warfare platforms that seek to disrupt its forces' communications, coordination, and target identification capabilities.[5]

The Alliance struggles with interoperability and C2 at the best of times; differing command styles, technology, capabilities, and terminology complicate communication among nations and within a blended chain of command. Standardization and basic military equipment compatibility challenges hinder NATO in peacetime; adversaries exploiting NATO's C2 vulnerabilities will only exacerbate these problems.

During the past year, Allies have started to adapt their operational concepts to address these challenges. The UK's Joint Concept Note (JCN) 1/20 for Multi-Domain Integration (MDI) focuses on 'integrating for advantage' across domains and levels of warfare, along with allies and partners.[6, 7] Similarly, the US JADC2 concept mixes new technologies and capabilities with adapted tactics, techniques, and procedures.[8] By examining Allies' newly proposed doctrinal solutions to the C2 problem, NATO can anticipate its own implementation challenges and identify key areas for future adaptation.

Preparing for the Future of C2

Effective C2 among Allies will require commanders and operators to operationally, if not necessarily technically, understand the cross-cutting nature of Multi-Domain Operations (MDO). NATO is already acting on this: its MDO C2 Demonstrator platform[9] acknowledges the existence of kinetic and non-kinetic threats to the Alliance and the impact of cross-domain effects.[10] NATO's Joint Warfare Centre (JWC) provides collective joint warfare training, and the North Atlantic Council (NAC) directed a Joint Effects function under the NATO Command Structure Adaptation (NCSA). Additionally, the Fires and Effects Synchronization Board addresses MDO challenges, including coordinating lethal and non-lethal effects through the NATO J-3.[11] Previously commissioned NATO studies, including SAS-085 and SAS-110, have endeavoured to nuance the Alliance's thinking about C2 relationships in complex environments, recognizing the importance of C2 agility[12] to account for diverse mission sets, command styles, and changing conditions within particular missions.[13] While these developments are promising, Allies are not advancing interoperable C2 systems rapidly enough, and NATO could do more to advance coordinating authorities for implementing MDO concepts.

Protecting shared understanding of the situational picture will be critical to enabling effective C2 of MDO; NATO should address critical cyber vulnerabilities in its Joint Intelligence, Surveillance and Reconnaissance (JISR) architecture. JISR provides timely information support including collecting, processing, and disseminating information across multiple domains from national assets.[14] Operationalizing an MDO concept will require NATO's JISR Task Force, Intelligence Fusion Centre, Joint Force Commands, and component commands to remain closely integrated to ensure that ISR is rapidly disseminated to strategic and tactical leaders.

Experimentation and subsequent exercises can begin to address changing C2 structures and improve readiness for future challenges. So long as C2 threats remain imminent, a robust experimentation program will be necessary to determine new approaches and uncover gaps, costs, and risks. NATO must also prioritize C2 experimentation across environments and scenarios.[15] When experimentation leads to new solutions and courses of action, continuously exercising NATO's strategic, operational, and tactical C2 will be necessary. NATO's Trident Juncture 2018 exercise and the US-led Defender Europe 20 enabled allies and partners to rehearse integrating C2 by rotating command responsibilities in different theatres with varying participants. However, as allies update their C2 structures and create command elements to absorb, NATO must prevent C2 becoming its Achilles heel. Training and exercises must incorporate complex denial scenarios that stress test C2 and specifically simulate operations amid degraded C2.

NATO has discussed developing an enterprise-wide architecture for its future C2 capabilities.[16] It should capitalize on technological innovations in Allies' ISR, Space, Cyberspace, and electromagnetic capabilities to bolster resilience. While some Allies are likely to take the lead on technological 'big bets,' NATO should look for ways to integrate national technological advancements for the wider Alliance's benefit. For example, the Alliance could experiment with technologies that gracefully degrade, or retain some function after critical processes are disrupted, or alternatively test new approaches that are more decision- and less data-centric.[17] Through NATO's Defence Planning Process, the Alliance should harmonize changing national plans and capability development, and could add graceful degradation-specific capability goals to its Minimum Capability Requirements.

NATO must also look beyond purely technical fixes to its strategy, operations, techniques, and procedures. Reliance on robust, high-bandwidth communications has been a hallmark of NATO operations, but these C2 channels will likely be disrupted in contested environments, requiring an appropriate mix of robust C2 capabilities and effective mission orders and tactics suitable for communications-denied environments. At a high level, NATO should consider new strategic or multi-domain operational concepts that address the challenges inherent in contested operating environments. From a US perspective, MDO nest under the concept of joint operations.[18] NATO joint staffs and the JWC could explore creating a NATO MDO concept to align joint warfare approaches across the Alliance.

New concepts may require new thinking about command authorities and authorizations. Determining the degree of autonomy that subordinates should possess to adapt to disrupted C2 and achieve the commander's intent in light of new member nation C2 plans is worth examining in the NATO context. The importance of C2 that is attuned to the environment and capable of shifting mid-operation should lead NATO leaders to consider decentralized command structures that empower staff to respond 'in the moment' more effectively.[19] For example, the US Air Force phrase 'centralized control, decentralized execution'[20] highlights the principle of decentralizing command to soldiers, enabling them to exercise decisions if cut off from the chain of command. Lower-level decision-making could improve speed, C2 agility, and effectiveness while more easily cutting across domains and joint force structures. Thinking about NATO C2 from the bottom-up may generate insights into best practices for survivability and linking distributed tactical nodes.[21] This approach must be inculcated into the professional culture to succeed and will require experimentation to determine relevant and potentially new practices.[22] For NATO forces to operate based on commander's intent amid degraded C2 conditions, doctrine, education, training, and exercises must adapt accordingly. US-led training with Allied forces could demonstrate how diffused C2 works in practice and could help Allies develop their own concepts.

Recommendations

As NATO grapples with greater C2 challenges, it can take several steps to improve its C2 resiliency.

First, the Alliance should consider adopting a NATO-wide MDO concept. A concept could help initially frame how to assess capabilities and determine roles in an interoperable C2 architecture. Wargaming and experimentation will be important for testing and validating the new concept, and red teaming and tabletop exercises can expose the seams between Allies and can highlight vulnerable nodes. This testing may also expose bureaucratic, technical, and cultural obstacles.

Second, when a concept is in place, NATO should conduct an Alliance-wide assessment to determine which Allies and partners are developing critical capabilities to support operators at C2 nodes. Allies must prioritize developing interoperable C2 systems with compatible equipment to mitigate gaps.

Third, NATO should establish common goals and criteria to measure progress towards interoperability and preparedness for C2 resilience. A 2013 US Joint Wargame assessing C2 in the context of the Air-Sea Battle concept identified unity of effort, flexibility, simplicity, resiliency, operational integration, and cross-domain synergy as performance indicators.[23] Future assessments should also include how C2 progresses during an exercise as it would during operations.[24] By adopting such goals and criteria, the Alliance can create benchmarks for measuring its progress and determining priorities based on need and ability.

Fourth, NATO will need to exercise for contested environments at scale to prepare for decentralized C2, test different force mixtures, and determine how best to exploit human-machine teaming and unmanned system advantages. It should exercise varied scenarios of C2 degradation and operations in denied environments. NATO will also need to reckon with the hard realities that decentralized C2 creates for coordinating wide-ranging MDO effects with limited communications. The US-led, multinational exercise Bold Quest is an example NATO could build upon in the future.

Preparing for the likelihood of degraded C2 is critical if NATO is to better prepare for future crises. Adversary efforts to disrupt C2 should not pitch the entire enterprise into the dark. Rather, resilient systems and agile, decentralized processes should enable Allies to take C2 attacks in stride. NATO must improve C2 resilience, interoperability, and compatibility of Allied C2 systems by investing in technology with graceful degradation capacity; adapting exercises and training to include denied environment scenarios; and exploring decentralized C2 doctrine. As technology has evolved, adversaries' opportunities for and ability to thwart NATO C2 has increased. NATO must start to strengthen its resilience for tomorrow.

Mr Owen Daniels is a research associate in the Joint Advanced Warfighting Division at the Institute for Defense Analyses in Alexandria, Virginia. He previously worked in the Scowcroft Center for Strategy and Security at the Atlantic Council and at Aviation Week magazine, and leads Young Professionals in Foreign Policy's Fellowship Program.

Ms Clementine G. Starling is a resident fellow and the deputy director of Forward Defense at the Atlantic Council. Starling's research focuses on great power competition with China and Russia, deterrence, US defense policy, and transatlantic security. Prior to joining the Atlantic Council, she worked in the UK House of Commons.

Endnotes

1. Kofman, Michael, 'It's Time to Talk about A2/AD: Rethinking the Russian Military Challenge,' War on the Rocks, 5 Sep. 2019 [Online]. Available: https://warontherocks.com/2019/09/its-time-to-talk-about-a2-ad-rethinking-the-russian-military-challenge/.
2. Schmidt, Andreas, 'Countering Anti-Access/Area Denial: Future Capability Requirements in NATO,' JAPCC Journal 23 [Online]. Available: https://www.japcc.org/countering-anti-access-area-denial-future-capability-requirements-nato/.
3. Williams, Ian, 'The Russia–NATO A2AD Environment,' CSIS, 3 Jan. 2017 [Online]. Available: https://missilethreat.csis.org/russia-nato-a2ad-environment/.
4. Dalsjo, R., Jonsson, M., Berglund, C., 'Don't Believe the Russian Hype,' Foreign Policy, 7 Mar. 2019 [Online]. Available: https://foreignpolicy.com/2019/03/07/dont-believe-the-russian-hype-a2-ad-missiles-sweden-kaliningrad-baltic-states-annexation-nato/.

5. Smith, Patrick, 'Russian Electronic Warfare,' American Security Project, Apr. 2020, pp. 3 [Online]. Available: https://www.americansecurityproject.org/wp-content/uploads/2020/04/Ref-0236-Russian-Electronic-Warfare.pdf.
6. UK Ministry of Defence, 'Multi-Domain Integration (JCN 1/20),' 2 Dec. 2020 [Online]. Available: https://www.gov.uk/government/publications/multi-domain-integration-jcn-120#:~:text=This%20integration%20must%20be%20across,domains%20and%20levels%20of%20warfare.
7. UK Ministry of Defence, 'Integrated Operating Concept 2025,' 30 Sep. 2020 [Online]. Available: https://www.gov.uk/government/publications/the-integrated-operating-concept-2025.
8. Hoehn, John, 'Joint All-Domain Command and Control (JADC2),' Congressional Research Service [Online]. Available: https://fas.org/sgp/crs/natsec/IF11493.pdf.
9. NATOC2COE, 'The NATO C2COE MDO C2 Demonstrator platform,' 11 Jun. 2020. [Online]. Available: https://c2coe.org/download/the-nato-c2coe-mdo-c2-demonstrator-platform/.
10. Freedburg, Jr., Sydney, 'Target, Kaliningrad: Air Force Puts Putin On Notice,' Breaking Defense, 17 Sep. 2019 [Online]. Available: https://breakingdefense.com/2019/09/target-kaliningrad-eucom-puts-putin-on-notice/.
11. Jones, M. and Diaz de Leon, J., 'Multi-domain Operations,' The Three Swords Magazine, 36/2020, pp. 40–41 [Online]. Available: https://jwc.nato.int/application/files/5616/0523/5418/issue36_08lr.pdf.
12. C2 Agility is the capability of C2 to successfully effect, cope with, and/or exploit changes in circumstances. C2 Agility enables entities to effectively and efficiently employ resources in a timely manner. NATO Task Group SAS-085 Final Report on C2 Agility, 2014 [Online]. Available: http://www.dodccrp.org/sas-085/sas-085_report_final.pdf.
13. NATO Task Group SAS-085 Final Report on C2 Agility, 2014 [Online]. Available: http://www.dodccrp.org/sas-085/sas-085_report_final.pdf.
14. Ferguson III, M., Harper, C., Hooker, R., 'Over The Horizon,' Atlantic Council, 14 Nov. 2019, pp. 3 [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/over-the-horizon-nato-joint-intelligence-surveillance-and-reconnaissance-in-the-baltic-sea-region/.
15. Ibid. 12.
16. Sirota, Sara, 'NATO to develop new air command and control capability architecture,' Inside Defense, 14 Jan. 2020 [Online]. Available: https://insidedefense.com/insider/nato-develop-new-air-command-and-control-capability-architecture.
17. Czarnecki, J., and Chamberlain, T., 'Graceful Degradation: A C2 Virtue for Our Times,' 18th ICCRTS, California: Naval War College, Aug. 2018.
18. Jones, Leon, 'Multi-domain Operations,' The Three Swords Magazine, 36/2020, pp. 38–41 [Online]. Available: https://jwc.nato.int/application/files/5616/0523/5418/issue36_08lr.pdf.
19. Tillman, M.E. and Conley. K.M., 'Designing and Assessing Command and Control to Deal with Complex and Ill-Structured Operational Environments'. In Operations Assessment in Complex Environments: Theory and Practice, edited by Adam Shilling. NATO STO, 2019.
20. Hinote, Clint, 'Centralized Control and Decentralized Friction,' Air University Air Force Research Institute, Mar. 2009 [Online]. Available: https://media.defense.gov/2017/Jun/19/2001764937/-1/-1/0/AP_0006_HINOTE_CENTRALIZED_CONTROL_DECENTRALIZED_EXECUTION.PDF.
21. Birch, P., Reeves, R., and Dewees, B., 'Building the Command and Control of the Future from the Bottom Up,' War on the Rocks, 16 Jan. 2020 [Online]. Available:, https://warontherocks.com/2020/01/building-the-command-and-control-of-the-future-from-the-bottom-up/.
22. US Marine Corps, 'MCDP-1 Warfighting,' Jun. 1997 [Online]. Available: https://www.marines.mil/Portals/1/Publications/MCDP%201%20Warfighting.pdf.
23. US Department of Defense, 'Air Sea Battle,' May 2013 [Online]. Available: https://archive.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf.
24. Ibid. 18.

© Airbus

Human-On-the-Loop

XIII

By Brig Gen (ret.) Jean Michel Verney, FR Air Force,
Col (ret.) Thomas Vinçotte, FR Air Force, and
Mr Laurent le Quement
Airbus Defence and Space

Introduction

In light of today's uncertainties, there is a shared realization that NATO's Air supremacy which has underpinned military operations since the 1980s is no longer a given. The playing field is being levelled due to an increasing number of peer and near-peer threats from resurging and emerging potential opponents. This is accompanied by a continued presence of asymmetrical conventional threats from rogue or failing states, or terrorist organizations. When facing such threats, two main trends can be observed. The proliferation of military capabilities, due to lower technological entry barriers, is leading to more denied environments, and spreading conflicts are overstretching NATO Air Forces.

Such challenges require a paradigm shift. Relying on the sole procurement of ever-increasing sophisticated fighter aircraft will only further reduce their numbers and availability. A more favoured approach is to speed up the information flow, between manned and unmanned platforms in varying sophistication, by linking fused sensor data to the most appropriate

Command and Control (C2) authority. Providing the right information in the right place at the right time will improve decision making in terms of speed and quality along the C2 cycles from the Air Component Command (ACC) to the tactical edge. Distributed decision-making is key to NATO doctrine. Contrary to past C2 approaches, the novelty lies in enriched data approaches where software, Artificial Intelligence (AI), automation, and satellite communication will bypass human limitations. As stated by General Terrence J. O'Shaughnessy, USAF (ret.), 'machine-enabled insights … can identify anomalous events, anticipate what will happen next, and generate options with associated repercussions and risks.'[1] This goes beyond implementing new cutting-edge technologies. Harnessing their full potential will require a doctrinal transformation, whilst ensuring adequate and meaningful human control.[2] This 'technological, doctrinal and ethical triptych' lies at the heart of any future combat Air system.

Adjusting to New Threats and Resulting Constraints

The increased likelihood of simultaneously facing peer or near-peer and asymmetrical opponents is imposing greater time constraints on NATO Air Forces. New threats are becoming increasingly agile and difficult to discriminate from their environment. This results in a decreasing amount of time available to execute a kill chain. Dealing with these threats in large-scale operations requires the parallel execution of many missions, as well as the simultaneous processing of huge amounts of data.

Furthermore, NATO Air Forces are also operating in more complex environments, as the need to avoid collateral damage and fratricide casualties remains the same. This is the prerequisite to keeping public support. Maintaining a certain level of 'cleanliness' in military operations requires an increasingly complex legal framework often difficult to translate into realistic and efficient operational guidance. The aim is not only to win the war but also the peace which follows. Hence, the scope of operations needs to be increasingly comprehensive, by considering all possible direct and collateral consequences of kinetic effects in terms of physical and psychological impacts. In such complex environments, complying with the ethical framework requires human involvement to ensure moral responsibility when manned and unmanned systems operate together.

Increasing Decisional Agility with Meaningful Human Control

This new environment, with its increasingly time-constrained and complex decision-making, calls for a strong adaptation of today's C2 model. The aim is twofold: regaining decision-making agility in terms of responsiveness and quality, as well as understanding and redefining the place of humans with regards to new information technologies. C2 is a process of implementing several decision loops in service of a strategy. It is now almost exclusively provided at command centres level such as Joint Force Air Component (JFAC) and Combined Air Operations Centre (CAOC) in a centralized mode, except for battle management which can be delegated to AWACS-like platforms.

Further accelerating the decision-making necessitates both the introduction of greater subsidiarity in the decision-making chain in a decentralized mode, and the provision of adequate decision support to the authority vested with C2 responsibility. To meet this dual challenge, this paper advocates that Battle Management, extended to multi-domains, should be conducted at all levels and when necessary down to the fighter aircraft. Distributed C2 in the cockpit will be enabled through the use of software and AI to assist pilots' decision-making by accessing and sorting through massive data, via satellite communications. Such C2 distribution to the tactical edge fulfils the need for greater responsiveness and control resilience. Deciding to do so depends on criteria linked to mission sensitivity[3] and situational awareness.[4] This need for control subsidiarity in large and contested environments implies a repositioning of humans in the decision-making loop, which can be examined through the conceptual notion of the Observe, Orient, Decide, Act (OODA) loop.

Currently, any C2 authority, benefiting from information management and synthesis tools or even the first bricks of AI applications, remains fully in charge of options development, solution choice, and execution. Such a semi-autonomous mode is called 'Human in the Loop (HITL)'.

Cockpits being complex high tempo environments, a fighter crew member, vested with control authority, will need solutions developed by AI under his or her supervision. The crew member will retain the prerogative to select another solution or refuse a specific sequence (veto). Such a supervised autonomous mode is named 'Human on the Loop (HOTL)'. The authors see this last mode as the basis for C2 subsidiarity at the fighter level, as it is the best fit to compensate for human weaknesses and machine limitations during the decision-making process. In most cases, a combination of 'In and On the Loop' modes will allow for a speedier C2 process.

The existence of the 'Human out of the Loop (HOOTL)' mode in which an AI develops and executes solutions without human intervention should also be noted. While this mode may appear at first inappropriate in terms of controlling an operation where human ethical and legal judgment is deemed crucial, there are extremely high tempo situations (e.g., anti-missile defence or very high-intensity engagement) where humans are no longer able to apply sound judgment. Only a rule-based AI application would be able to exercise time-limited task control. A prerequisite being that this application follows vetted design and testing protocols through a normative process, including a massive recourse to simulation to ensure appropriate ethical and legal adherence. This last mode should remain exceptional but possible in view of an 'exceptional but defined situation'. This normative process to ensure the trust and reliability of AI is obviously also required for 'In and On the Loop' modes. This robust adaptation of the C2 model on the principle of distributed multi-domain control with new AI-assisted 'On the Loop' authorities at the tactical edge constitutes the condition for successful agile decision-making when facing increasingly contested environments.

Requiring a Technological and Doctrinal Revolution

This new paradigm shift is made possible by the advent of large bandwidths, big data, and AI allowing varying degrees of autonomy. It will require an in-depth review of techniques, tactics, and procedures to assume control responsibilities. To illustrate this, one must focus on two areas of innovation: the Multi-Domain Combat Cloud (MDCC) and doctrine at the tactical level.

Firstly, there is currently an Information Technology and Communications structure in development capable of managing massive flows of information from the five domains (Land, Air, Sea, Cyberspace, and Space) and supporting decision-making in terms of control for collaborative multi-domain combat. The framework for this structure is the 'service oriented' C3 NATO Taxonomy. The objective is to emerge from a patchwork of stove-piped systems at work within different communities and which hinder the integration of military effects. An MDCC, based on this 'service oriented' approach, will be capable to support the C2 process.

The result is the provision of shared services between all C2 players, feeding applications embedded in various systems (Air Command and Control System, Alliance Future Surveillance and Control, or fighter aircraft) and enabling dynamic distribution of control. These applications will cater for the operational needs and offer warfare software suites and/or AI-based solutions with varying degrees of autonomy. As previously explained at the fighter aircraft level, these applications mainly fall under a 'HOTL' mode with an AI providing battle management options in compliance with the rules of engagement (legal framework), and with the possibility of human vetoing to ensure the meeting of ethical requirements. In this process, the concepts of AI confidence and its traceability[5] will be crucial and will require specific C2 authority training during simulation sessions to be properly mastered. Likewise, if the use of AI-based on automated systems and pre-established rules seems acceptable for C2, real-time employment of machine and deep learning AI-based on autonomous systems is probably not desirable due to unpredictable proposed solutions potentially at odds with human ethics. However, usage could be possible after AI validation through the previously mentioned normative process. It is still too early to set precisely the limits and types of AI in the field of C2. The very sensitivity of this decision-making process, which ultimately comes under the responsibility of humans, calls for a cautious approach even though in any military campaign, the notion of human control already results from human judgment.

Secondly, one has to focus on doctrinal aspects and in particular, the possibility of multi-domain control delegation at the fighter level. To do so, the authors used as a basis the current Tactical Battle Management Functions (TBMF) within NATO. TBMFs already allow specific tasks' delegations to the AWACS level and even down to the fighter but solely for Air defence. It appears that the very nature of these TBMFs based on situational awareness sharing, coordination of activities, concentration of efforts in several domains (Land, Air, and Sea) and a shorter decision cycle are relevant for broader C2 distribution. Consequently, in view of new threats and the need to multiply possible military options (notably the search for mass effect), the authors' work has resulted in a formalized extension of these TBMFs to all Air operations around the principle of 'multi-domain collaborative combat'. These new TBMFs have been designated as MDTFs (Multi-Domain Tactical Functions) and outline a possible doctrinal framework for the 2040 horizon (as shown in Figure 1).

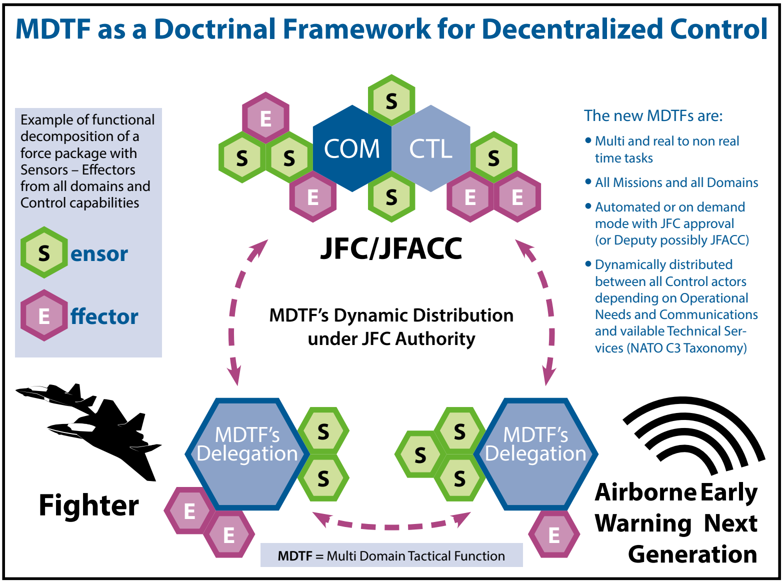

MDTF as a Doctrinal Framework for Decentralized Control
Example of functional decomposition of a force package with Sensors – Effectors from all domains and Control capabilities
S ensor
E ffector
COM
CTL
S
E
JFC/JFACC
MDTF's Dynamic Distribution under JFC Authority
MDTF's Delegation
MDTF's Delegation
Fighter
Airborne Early Warning Next Generation
MDTF = Multi Domain Tactical Function
The new MDTFs are:
• Multi and real to non real time tasks
• All Missions and all Domains
• Automated or on demand mode with JFC approval (or Deputy possibly JFACC)
• Dynamically distributed between all Control actors depending on Operational Needs and Communications and vailable Technical Services (NATO C3 Taxonomy)

Figure 1: *Multi Domain Tactical Functions.*

Above all, MDTFs provide the doctrinal framework for C2 distribution through the MDCC at the most appropriate level and in real-time, depending on the operational needs, the available platforms, the state of communications, as well as the workload transfer needs between the various C2 players. To summarize, these MDTFs make it possible to carry out a permanent redistribution of the OODA loops and to reconstruct the design of force packages according to the operational constraints.

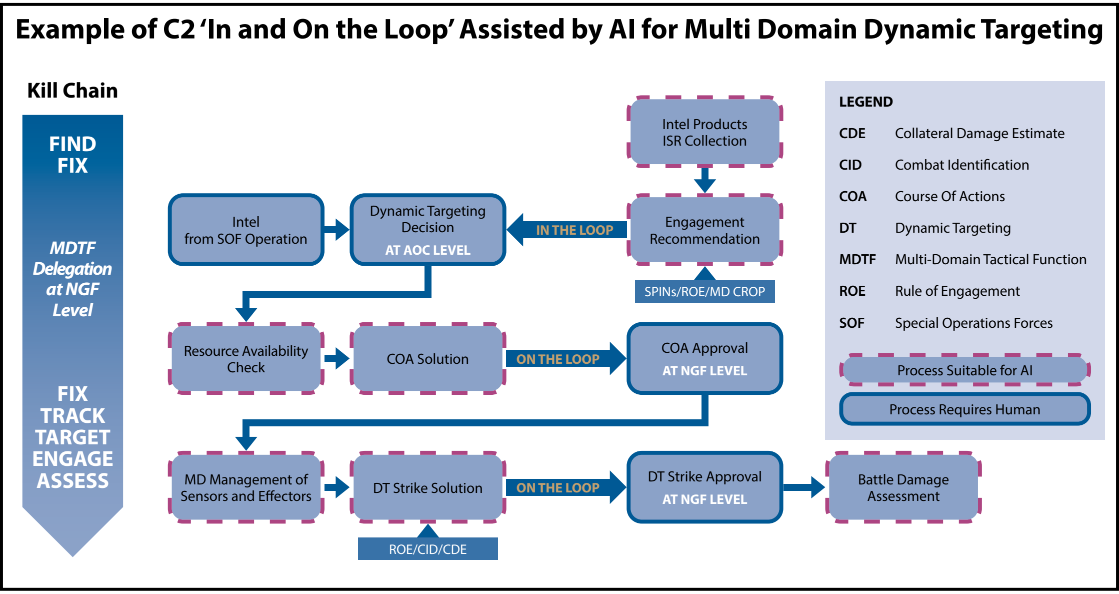


Figure 2: *Example of C2 In and On the Loop.*[6]

This combination of 'Tactics & Techniques & Procedures provided by the MDCC and the MDTFs is illustrated through a multi domain dynamic targeting kill chain supported by AI applications and a combination of 'Human in/on the Loop' modes.

Figure 2 shows a notable acceleration of the decision-making process through C2 delegation and a functional decomposition of force packages no longer based on functions aggregated on a single platform but on the combination of functions from all available platforms. This new approach will pave the way for highly tailored and faster multi domain kill chains.

Conclusions

A strong link exists between the amount of information to be processed, the tempo and the position of humans in the decision process. The faster it goes, the more humans will be 'On the Loop'. Hence, any decision regarding Battle Management, taken in a fighter aircraft, should mostly be 'On the Loop'. Nevertheless, 'In the Loop' has its virtues in well-staffed environments where the temporal pressure is lower and the C2 authority is more familiar with the potential options to be decided. Hence, C2 will require mostly a combination of 'In and On the Loop' modes.

As there are no evident ethical issues with the 'On the Loop' mode when supported by trusted and reliable AI, significant C2 delegations can be given to properly-equipped new generation fighter aircraft to speed-up the decision process where there is a specific need for reactivity and resilience. These delegations will be allowed through the MDTFs supported by the MDCC. Efficiency and adherence to ethical standards can both be achieved.

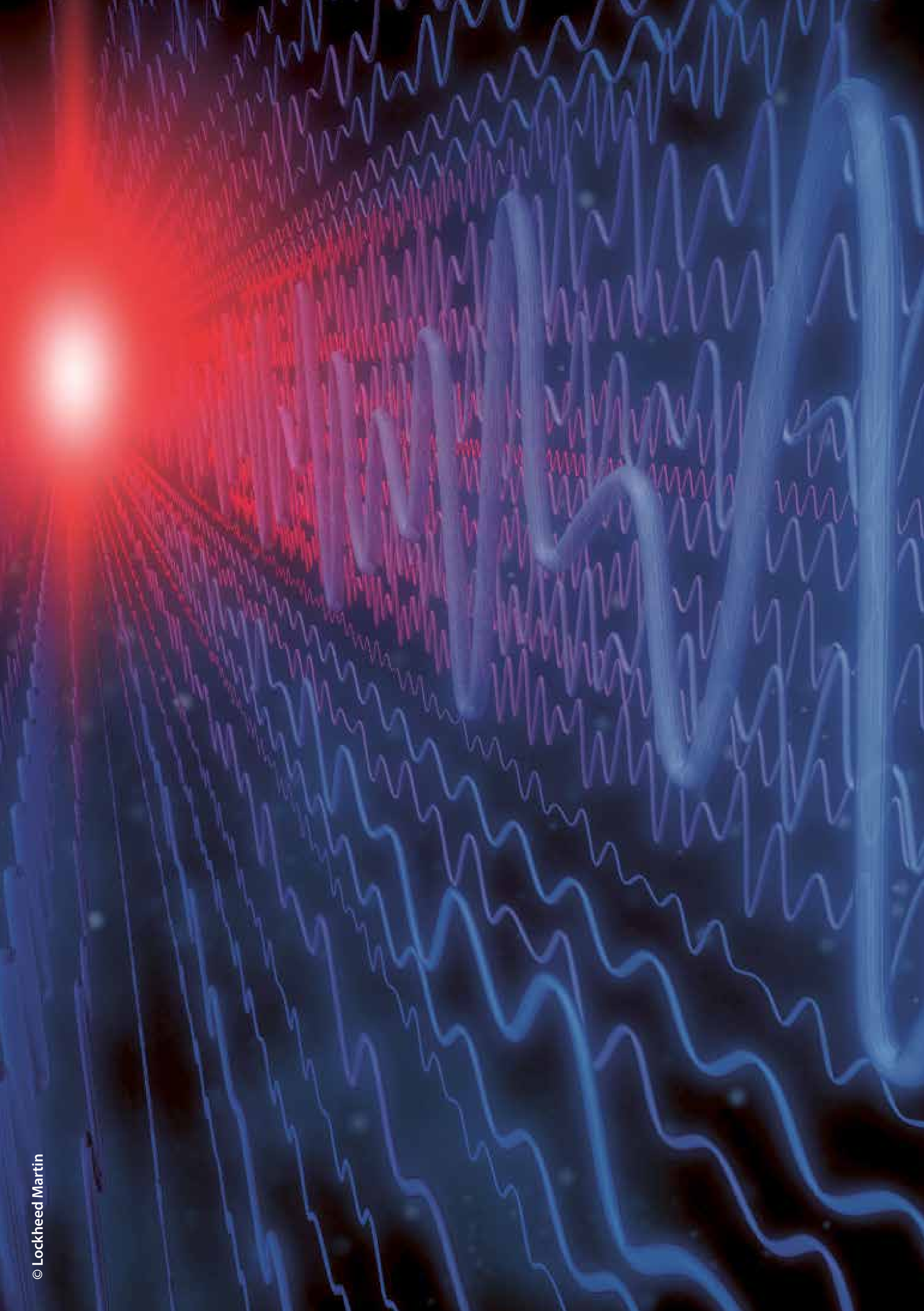
Brigadier General (ret.) Jean-Michel Verney (FR Air Force) graduated from the FAF Academy in 1987 and the US Air War College in 2003. He has 3,000 flying hours (Jaguar, Mirage 2000D) with 122 war missions and C2 expertise as a HQ officer. He joined Airbus in 2017 as a FCAS Operational advisor.

Colonel (ret.) Thomas Vinçotte (FR Air Force) graduated as a French Air Force fighter pilot in 1987 and from the Ecole de Guerre in 2003. He has over 3,300 flying hours (Jaguar, Mirage F1CR, Mirage 2000 RDI & Mirage 2000-5) with 83 war missions including one ejection and C2 expertise as a HQ officer. He joined Airbus in 2019 as a FCAS Senior Operational Advisor.

Mr Laurent le Quement graduated from Aston University in 1996. He worked in automotive and transformation consulting before joining Airbus' launcher division in 2010. He held numerous positions in business development and innovation before becoming FCAS Head of Marketing in 2018.

Endnotes

1. Terrence J. O'Shaughnessy, Decision Superiority Through Joint All-Domain Command and Control, Joint Force Quarterly, no. 99 (2020).
2. 'Control' is employed in the sense of 'Command and Control'. It is the same throughout the document.
3. Assessing the sensitivity of a situation is usually based on the following parameters: risk for own crews, risk of collateral damages and risk on the rest of the campaign.
4. Assessing who has the best perception position.
5. Knowledge of the field of possible solutions as well as of algorithmic type sequences.
6. Adaptation of figure provided page 22 in Joint All-Domain Command and Control for Modern Warfare Report, RAND CORPORATION, Mar. 2020.



© Lockheed Martin

Superiority in the Electromagnetic Spectrum – Panel Introduction

XIV

With an Emphasis on Electronic Warfare

By Maj Andreas Wurster, GE Army

Joint Air Power Competence Centre

'The EMS is the cross-domain and fundamental glue which binds the other operating domains of Air, Land, Maritime, Cyber, and Space.'[1]

Introduction

The Joint Air & Space Power Conference 2021 will offer a platform to reflect upon various aspects of delivering NATO Air & Space Power at the Speed of Relevance. One of these aspects is the challenge for the Alliance to achieve operational superiority in the Electromagnetic Spectrum (EMS) using different means. One important pillar in this effort is the support of all divisions of Electronic Warfare (EW): Electronic Countermeasures, Electronic Protective Measures and Electronic Warfare Support.[2]

Due to NATO support for missions in the fight against terrorists and non-state groups since the beginning of the century, the subject matter has been pushed out of the focus of the Alliance. Opponents like the Taliban in Afghanistan or Islamic State of Iraq and Syria (ISIS) are only rudimentarily able to operate in the EMS. This situation changed in 2014, due to the illegal and illegitimate annexing of Crimea by Russia and the ongoing wide-ranging military build-up in the Black Sea Region. These events showed that Russia has become an increasingly capable adversary of NATO. Russia has focused on developing and deploying a vast array of EW systems in this area. The ongoing Conflicts in Ukraine and Syria have also confirmed the already presumed importance of EW in Russian military operations and the necessity for NATO to enter this competition.[3] China, the other rising power in the world,[4] has been focused on developing EW capabilities and training to operate in a complex Electromagnetic Environment (EME) since the early 2000s. In the past few years, the Chinese People's Liberation Army (PLA) deployed EW and Signal Intelligence (SIGINT) capabilities, which is the Intelligence derived from electromagnetic signals or emissions,[5] on the seven island-reef outposts in the South China Sea.[6] This has demonstrated the requirement for NATO to keep pace with the developments in this sector. All of these developments have been recognized by NATO and have triggered an alignment of the Alliance's mindset and strategy in this sector.

The Intangible EMS

The EMS, as the range of frequencies of electromagnetic radiation, is a fundamental component of the natural environment. The EMS includes radio waves, microwaves, heat radiation, visible light, ultraviolet radiation, x-rays, electromagnetic cosmic rays and gamma rays.[7] The EMS is the foundational medium of the EME, which is the totality of electromagnetic phenomena existing at a given location.[8] The military term for this is the Electromagnetic Operational Environment (EMOE), which is the space in which military functions are performed.[9] In modern warfare, EMS superiority is a leading indicator and fundamental component of achieving superiority in

Air, Land, Sea, Space or Cyberspace. The EMS not only provides the critical connective tissue that enables all-domain operations but represents a natural seam and critical vulnerability across joint force operations.[10]

VISION: Freedom of Action in the Electromagnetic Spectrum and How to Manage That

When dealing with the battlefield of the future, most agree that such a battlefield extends over all domains: Air, Land, Sea, Space and Cyberspace, which must be connected to enable effective and resilient C2. This connection between the domains can be achieved exclusively through the EMS. For NATO, the EMS is an essential part of military operations, so much so that many Allied leaders now see the EME as an operational environment and a part of the battlespace where friendly forces manoeuvre in time, location, and spectrum to create electromagnetic effects in support of the commander's objectives.[11] NATO EMS Strategy aims to exploit, access, and control the EMS where and when needed to achieve NATO Military Strategic objectives and ensure that it will remain the superior military force, postured to take advantage of the EMS with the ability to exploit, mask, and manoeuvre within a congested and contested EME. The strategy's overarching goals are: (1) institutional awareness and advocacy, (2) effective joint EMO, and (3) robust EMO capabilities. EMO includes any type of activity which deliberately transmits and receives electromagnetic energy in the EME for military operations.[12]

The EW Contribution

EW, which is the military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects, has been the traditional warfighting element within the EMS since the beginning of the 20th century. Today, a tremendous technological revolution has led to the emergence of new advanced capabilities and functions in the EME such as Directed Energy Weapons (DEW) and low emission radars.[13] In the context of Alliance defence, potential adversaries have significantly more capabilities in the field of EW than terrorist groups and possess the ability to impact not only the Alliance military forces, but also the civilian populations upon whose will Alliance cohesion depends. Therefore, NATO recognizes EW capability as an essential tool for the full spectrum of operations and other tasks undertaken by the Alliance.[14] Within NATO, this effort is led by the NATO Electronic Warfare Advisory Committee (NEWAC) which is responsible for overseeing the development of NATO's EW policy, doctrine, and command and control concepts as well as monitoring EW support to NATO operations.[15]

The 'Cyber' Part of the EMS

Cyberspace has become an attractive domain of operations for power projection. It is the only domain which has been created by humans and is exclusively accessible over the EMS (e.g. copper wires, fibre optic cables, and microwave and satellite relays).[16] NATO, in 2016, declared Cyberspace an operational domain giving the Alliance significant opportunities and also confronting the Alliance with serious challenges. In the context of collective defence, it is essential to ensure resilience against enemy bot and algorithm-attacks in the grey zone, where the line between war and peace is more blurred. Competition short of open conflict is increasingly becoming the norm, and NATO must maintain the ability to command and control operations during a conflict or crisis. The challenges for NATO and individual member states can be summarized in how they preserve freedom of action and achieve strategic and operational advantage in and through EMS, taking into consideration legal implications, technical feasibility, and especially human factors. NATO can best address these challenges if they are tackled by the Alliance and the member states in cooperation with industry and academic partners.

Conclusion

As the theme of the 2021 conference suggests, 'delivering NATO Air and Space Power at the Speed of Relevance' must be ensured. To achieve this goal, it is incontestable that the speed and reliability of data transmission within the EMS for all Alliance's issues across all domains is the key to success.

The following articles will introduce the reader to some important aspects of these challenges which will be the focus of a panel discussion during the JAPCC Conference:

- ACM Sir Stuart Peach (UK Air Force) provides a Senior Leader's Perspective regarding the EMS, EW and Cyberspace. In his article, ***NATO Electronic Warfare and Cyberspace Resilience***, he derives the necessity for NATO to achieve its vision of Cyberspace and EMS exploitation, access, and control when and where needed to achieve Alliance objectives.

- The next article, ***Speeding Up the OODA Loop with AI***, is written by Mr Owen Daniels. In the piece the author examines both conceptual and technological challenges to the Observe, Orient, Decide, and Act Framework, as well as potential implications for Alliance militaries.

- Lieutenant Colonel Paul J. MacKenzie (CA Air Force) outlines the relevance of ***Cyberspace in Cyberspace and Joint Air and Space Power***. The author presents the importance of cybersecurity in particular, from the early and slow-moving stages of Air and Space systems Research and Development (R&D) to how activities in these phases can eventually influence the Air and Space power capability gaps with potential adversaries.

- In ***Electronic Protective Measures*** Mr Dirk A. D. Smith and Mr Steve Tourangeau examine the importance of terms within the subject area of EW. The article addresses the confusion with the terms Electromagnetic Protection (EP) and Defensive Electromagnetic Attack (DEA). The authors clears-up the definitions through examples of each and makes the obvious suggestion of what needs to be done.

- Then, Mrs Melinda Tourangeau describes in her article, ***Managing the Electromagnetic Spectrum***, NATO's dependence on the EMS. She describes the access to the EMS on its way to becoming a global public goods resource like clean water, safe food sources, and responsible industrial waste management. The confluence of disparate issues across a singular public good presents what is classically called a Large-Scale Collective Action Problem (L-SCAP), which the author discusses in more detail in her article.

- The final article, ***Security Convergence for Air and Space Power***, comes from Colonel Eric D. Trias and Colonel Martin L. Rothrock (US Air Force). The authors address the concept of security convergence of the three protection disciplines, namely physical, cyber, and Continuity of Operations (COOP).

Major Andreas Wurster (GE Army) is the Subject Matter Expert for Intelligence in the JAPCC. He graduated a two-year study in economic computer science at the Bundeswehr College for business and computer science. He has an Intel-SOF and airborne background and was deployed three times on NATO missions in Afghanistan.

Endnotes

1. Willis, Matthew and Stathopoulos, Panagiotis, 'The Necessity of Integrating the Electromagnetic Spectrum's Disciplines Under a Single Domain of Operations', JAPCC Journal, no. 30 (2020): p. 72–77.
2. NATO AAP-06, 'NATO Glossary of Terms and Definitions', Edition 2020, p. 47.
3. Smith, Patrick, 'Russian Electronic Warfare, A Growing Threat to U.S. Battlefield Supremacy', American Security Project (ASP), https://www.americansecurityproject.org/wp-content/uploads/2020/04/Ref-0236-Russian-Electronic-Warfare.pdf, accessed 26 Mar. 2021.
4. Stoltenberg, Jens, 'NATO Secretary General's Press Conference following the meeting of the NACinLondon, 3–4 Dec. 2019', https://www.nato.int/cps/en/natohq/opinions_171554.htm, accessed 25 Feb. 2021.
5. Ibid. 2., p. 118.
6. Dahm, J. Michael, 'A survey of Technologies and Capabilities on China's Military Outposts in the South China Sea', Johns Hopkins University, https://www.jhuapl.edu/Content/documents/EWandSIGINT.pdf, accessed 26 Mar. 2021.
7. Ibid. 2.
8. Ibid. 2., p. 46.
9. Ibid.
10. US Department of Defense, 'Electromagnetic Spectrum Superiority Strategy' Oct. 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2397850/electromagnetic-spectrum-superiority-strategy-released/, accessed 26 Mar. 2021.
11. von Spreckelsen, Malte, 'Electronic Warfare – The Forgotten Discipline', JAPCC Journal, no. 27 (2018): p. 41–45.
12. Ibid.
13. Stathopoulos, Panagiotis, 'The Dimension of the Electromagnetic Spectrum', Joint Air & Space Power Conference 2020 Read Ahead: p. 111–117.
14. NATO Topics, Electronic Warfare (last updated Nov. 2016) https://www.nato.int/cps/en/natohq/topics_80906.htm, accessed 23 Feb. 2021.
15. NATO Topics, The 107th NEWAC convenes in Brussels (last updated Nov. 2019) https://www.nato.int/cps/en/natolive/news_171280.htm?selectedLocale=en, accessed 23 Feb. 2021.
16. Ibid. 1.

Policy and Strategy

Dynamic C2 Synchronized Across Domains

Superiority in the Electromagnetic Spectrum

NATO Space

© NATO; Shield background: Pasko Maksim/Shutterstock.com

NATO Electronic Warfare and Cyberspace Resilience

XV

By Air Chief Marshal Sir Stuart Peach GBE KCB ADC DL, UK Air Force

Chairman, NATO Military Committee

Any organization needs to adapt to survive. NATO is no different. In the last two years working closely with the NATO Chiefs of Defence, our Alliance has delivered the first NATO Military Strategy since the 1960s. This provides the framework for NATO as a military Alliance. Supreme Allied Commander Europe (SACEUR) is delivering the Deterrence and Defence for the Euro-Atlantic Region Concept and SACT is leading on the delivery of the NATO Warfighting Capstone Concept, which formalizes our approach to the future via a structured warfare development agenda.

NATO's component commands have been equally busy in preparing and adapting for the future, as have some of our Centres of Excellence. Under the leadership of General Harrigian, the JAPCC is developing concepts such as Joint All-Domain Operations, which includes the Electromagnetic Spectrum (EMS) and Electronic Warfare (EW), which help keep NATO strong and fit for the future. Our Alliance continues to adapt, as it has done for more than 70 years, to defend and deter across all domains.

As a strong supporter of the JAPCC, I am especially delighted to be able to contribute some thoughts ahead of the 'NATO EMS Emphasizing Electronic

Warfare' Panel. These are essential topics for NATO and support our thinking on how to understand the requirements, the shortfalls and how to work together to address both.

In recent years, NATO has had to adapt to face new challenges presented by the rapid advancement of technology, some of which are non-conventional, such as cyber or hybrid threats. These threats have become transnational, non-attributable and in some cases, low-cost. Those who want to harm us are using them. They are not 'emerging,' they are in use. So disruptive technologies influence the modern security environment; therefore keeping up with the rapid pace of technological change remains one of the biggest challenges for our Alliance.

Potential opponents are focusing on developing Cyber and EW capabilities, as they represent relatively 'low-cost' and asymmetric ways to impact or dominate operational domains. Russia and China have been particularly active in Cyber and Electronic Warfare, and are exploiting the Electronic Magnetic Spectrum to great effect. By observing Russia's ongoing cyber and electronic warfare actions, as well as China's evolving strategies, the West, including NATO and its allied militaries, need to be able to counter these capabilities.

The combined experience and strategies of our Nations are shaping NATO's view on Cyberspace, the EMS, and EW disciplines. Additionally, the number of nations actively developing new approaches and capabilities in these fields demonstrates the collective understanding that exploiting the Cyberspace domain and electromagnetic environment for military advantage is vital to achieving military objectives across our range of operations. The trick is to evolve coherence, spot opportunities and innovate.

Not only has this helped our Alliance build a response, but it helps strengthen interoperability in Cyberspace and EW among Allies and

Partners. Interoperability remains a key enabler for NATO and facilitates meaningful contributions from all Allies and Partners to its core tasks. Improving our interoperability provides significant cost benefits to NATO Nations as members pool and share resources. Our Alliance is the convening authority for Cyberspace and EW to enable interoperability in response to these emerging threats; we should act like it.

Each of the military operational domains are inextricably linked. In order to deter aggression, NATO must demonstrate its ability to act simultaneously across Land, Sea, Air, Space and Cyberspace. Cross-domain deterrence invariably involves the use of threats in one domain to counter activities in other domains. In the future, the interdependencies between domains will continue to grow, much like what we have seen with the use of hybrid tactics. Countering hybrid actors and activities calls for a comprehensive and coordinated response in multiple domains, which means NATO must start considering deterrence and defence across all domains through a multi-domain warfighting approach. This has re-emphasized the need for NATO to move beyond 'joint operations' and start thinking and acting in a multi-domain environment.

I have made clear our calling for a renewed focus on improving proficiency in our Cyberspace and Electromagnetic Spectrum Operations: by building awareness, developing policies and strategies, acquiring new capabilities, working with industry and academia, and training our people to become experts.

Often our military leaders highlight the critical role that Cyberspace, the EMS, and EW play in warfare within all operational domains to remind Alliance decision-makers of their importance. And we see other actors in this arena making the case for us. The many attacks and displays of cyber and EW activities in the last few years – especially prominent during Russia's illegal annexation of Crimea, but also widely in use throughout the

COVID pandemic – spurred NATO Nations back into action with the largest reinforcement of NATO's collective defence in a generation, including in the fields of cyber and EW.

In Cyberspace, NATO has established a roadmap to Cyberspace as an operational domain approach, with activities along the following lines of effort: training, capability development, organizational constructs, operational planning, exercises and strategic communications. We have reinforced our hybrid and cyber defences by establishing Counter-Hybrid Support Teams and a Cyberspace Operations Centre.

The use of the word 'deterrence' in connection with Cyberspace is significant, because it is another step towards the acceptance of offensive cyber capabilities as part of collective defence. NATO has agreed to integrate national cyber capabilities or offensive cyber into allied operations and missions. We have continued to build our resilience by updating our baseline requirements for national resilience, such as energy, transport, and communications, including the impact of 5G and other new technologies. We also address threats from Cyberspace; the security of supply chains; and foreign ownership and control of infrastructure. All of this will make NATO more effective and resilient in Cyberspace. This work is urgent.

In order to continue adapting to the changing security environment, NATO is developing better policies and doctrines. Amongst others, the 2019 NATO Military Strategy, provides us with overarching military guidance that sets out NATO's military priorities and approach to current and future threats, and guides commanders on tasks to maintain our security. Our thinking has fundamentally shifted from capability-based assessments to threat-based assessments. We are intelligence-led and threat informed. Building on the military strategy, two concepts have been developed. First, the concept of the Deterrence and Defence of the Euro Atlantic area (DDA), which brings together current military thinking as we face a more unpredictable world and deal with the consequences of a changed security environment. The DDA is supported by the NATO Warfighting Capstone Concept, which looks forward 20 years and sets a vision to support Allies' efforts to develop the Alliance's Military forces. The concept will identify potential capability gaps and provide the necessary recommendations to ensure NATO exploits opportunities and innovative approaches, including the use of emerging and disruptive technologies, to maintain its military advantage. This work is essential for maintaining NATO's military edge and ensuring that our capabilities remain fit for the future. We must also consider new technologies to enable our defence in the digital age, and in the age of artificial intelligence. Crucially, these concepts steer the resource plans that are required to make this a reality.

NATO continues to research, develop, test, and train new capabilities as well as develop and refine our tactics. Thanks to the work done thus far, our Alliance has already been acquiring some of these capabilities. NATO's fleet of AWACS aircraft will undergo a modernization effort, valued at 1 billion US dollars, providing the fleet with sophisticated new communications and networking capabilities. It will ensure that NATO AWACS continue to be our 'eyes in the sky', supporting our operations until 2035. NATO will also acquire over 1 billion euros worth of satellite capacity in 2020–2034. This is NATO's largest investment in satellite capacity. It will help our forces communicate with each other more securely and more quickly. We have a Space Centre, which will grow. Allies will also be able to share information gathered by remotely piloted platforms. In addition, NATO will move ahead with 1.4 billion euros of investment in new technologies in areas ranging from cybersecurity to surveillance and reconnaissance. Earlier this year, SACEUR declared NATO's fleet of new Alliance Ground Surveillance aircraft initially operationally ready to conduct missions. This is a major milestone for the programme. We have a Joint Enterprise for Intelligence, Surveillance and Reconnaissance. With a reset on EMS/EW, NATO is on the right track, but in an unpredictable world, we cannot let our guard down. NATO is determined to stay ahead of the technological curve.

However, for NATO to be successful in its deterrence and defence posture, it must harness both traditional and non-traditional technologies, including innovation from the civilian sectors. Today, most advancements in technology are driven by the commercial sector rather than the public defence sector; industry now far exceeds military investments in research and development. Readily available cutting-edge components produced by the civilian sector allow our military research and development to leverage commercial-scale production and thus prioritize the development of military-essential components without the duplication of work. NATO understands the benefits of working with subject matter experts and start-ups, their expertise is crucial for NATO to remain agile and capable; we need to make it easy for them to work with us.

More advanced technologies and better interoperability can improve NATO's overall efficiency throughout Cyberspace and the EMS. While, heavily investing in new capabilities, NATO is also looking at our existing courses to identify any types of gaps and overhaul the individual training opportunities. We are also increasingly incorporating cyber and EW in our exercises. Locked Shields, Cyber Coalition, Trident Juncture, Unified Vision, and NEMO exercises all have cyber and EW components, so allied and partner troops can observe their effects in real life, and practice countering them.

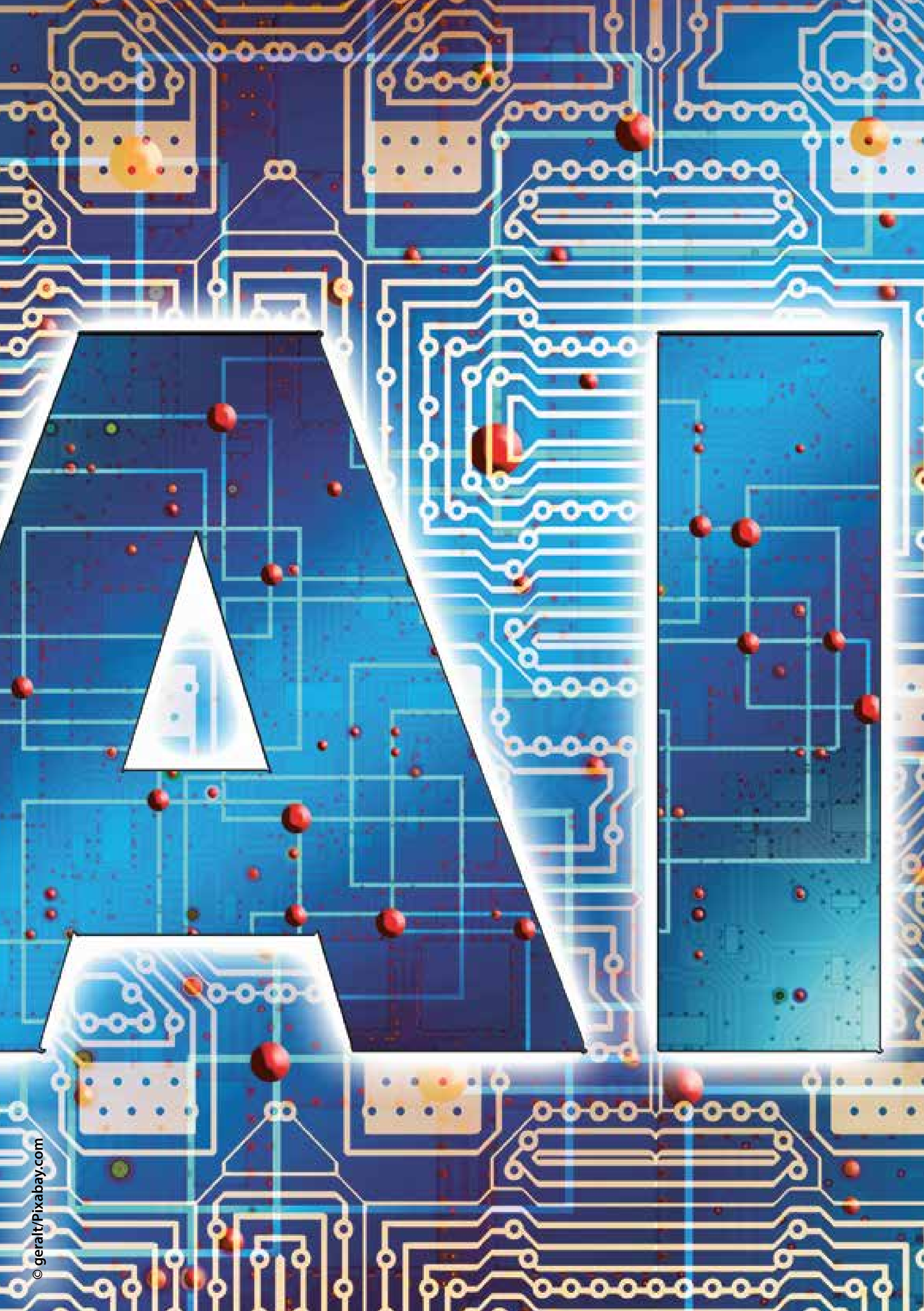
NATO is aware of the opportunities, challenges, and threats posed by cyber and EW. We are working together to achieve an edge, be it by increasing our defence spending, investing in better capabilities, improving the institutional awareness of our leadership, educating and training our troops in realistic scenarios, developing supporting policies and strategies or building our interoperability.

However, we must also consider that to provide a credible military advantage, the people, processes, and systems of the future must be able to operate in a complex, multi-domain, cross-organizational and multinational environment, to deliver needed effects through the superior employment of EMS, EW, and Cyberspace capabilities. Therefore, we must aim for NATO to achieve its vision of Cyberspace and EMS exploitation, access, and control when and where needed to achieve Alliance objectives.

For over 70 years, NATO has protected our populations, by learning from the changing security environment and continuously adapting to existing and emerging challenges. By engaging together as an Alliance of 30 Nations, on complex topics related to Cyberspace and EW, we all benefit.

As we have demonstrated time and time again, NATO's success rests in its ability to continuously adapt to a changing world and a shifting security landscape. We will continue to do so to guarantee the security of all of our Allies.

Air Chief Marshal Sir Stuart Peach (UK Air Force) is the 32nd Chairman of the Military Committee of NATO. He is NATO's most senior military officer and is the Military Adviser to the Secretary General and the North Atlantic Council. He attended the University of Sheffield (BA), University of Cambridge (MPhil in International Law and International Relations), RAF Staff College and the Joint Services Command and Staff College (HCSC). He holds four honorary Doctorates from UK Universities: Hull, Kingston, Sheffield and Loughborough, in Technology and Letters (DTech, DLitt).



© geralt/Pixabay.com

Speeding Up the OODA Loop with AI

XVI

A Helpful or Limiting Framework?

By Mr Owen J. Daniels
Institute for Defense Analyses

Strategists, warfighters, and technologists have heralded Artificial Intelligence (AI) as a potential tactical and strategic tool for outpacing adversary decision-making processes, commonly seen through the frame of the OODA (Observe, Orient, Decide, and Act) loop. Conventional thinking posits that human-machine teams augmented by AI-enhanced technologies will be able act more *quickly* than opponents in a conflict, gaining decisive advantages that could enable victory. Amid competition with near-peers who can access similar capabilities, enthusiasm for exploiting AI technology across kinetic and non-kinetic domains is understandable: consistent advantage over the adversary to act and react more quickly could prove decisive.

Yet conceptualizing AI use through the OODA loop's emphasis on speed ignores the limitations of this heuristic framework and the complexity of human-machine teaming, and may stunt creative thinking about AI's current military applicability. By over-generalizing AI's advantages only in terms of speed, stakeholders could inadequately explore how AI could help militaries. Focusing on speed also de-emphasizes potential risks like inadvertent escalation, un-explainability behind AI decisions, training and data issues, and legal or ethical concerns.

Discussion around future AI use needs to be grounded in specificity, rather than treating AI as a panacea for warfighting challenges. Distinguishing between types of AI, general versus narrow AI or traditional machine learning versus deep learning systems, is key to ensuring precise terminology and demystifying conversations about AI's military applications. For example, structured applications of AI in non-warfighting, support functions may present the best near-term application of the technology. While recognizing AI's great potential for certain military applications, this article highlights some flaws in the discourse around military AI use and offers several key lessons.

Conceptual Challenges with OODA Framing

US Air Force Colonel John Boyd developed the OODA loop framework as an advantageous mental model for fighter pilots trying to win direct Air-to-Air encounters with symmetrical circumstances. The continuously operating loop segments the decision cycle into the aforementioned subcomponents and accounts for the pilot's previous experiences, training, and culture. Boyd posited that pilots who could cycle through their OODA loops more quickly, observing situational changes, orienting to understand new information, deciding on a course of action, and acting on it, could dominate opponents.[1] In that context, with limited inputs and a relatively constrained environment, the OODA loop offered an appealing heuristic model.

The straightforward logic and explainability of Boyd's model have led militaries, businesses, and technologists to adopt and apply the OODA loop beyond its original context.[2] Recently, the OODA loop has emerged as a popular framing device for discussing how AI could help militaries function at greater speed.[3] In discussions of great power competition, the OODA loop provides an easy, surface-level comparative framework among near-peers who might use AI technologies in similar ways.[4] Emerging military concepts that feature AI, like the US Air Force's Joint All-Domain Command and Control system, are described as having 'information over the OODA loop … at the heart of successful execution.'[5] One research team even identified AI as the latest advancement to replace the human element of the OODA loop with technology in that AI might transform human decision-makers' abilities to orient by integrating and synthesizing massive, disparate information sources alongside new manoeuvre and fires technologies for acting, as well as digitization technologies to improve observing and disseminating information.[6] Others theorize that AI may one day be authorized to make lethal battlefield decisions at a pace far exceeding that of humans.[7]

AI's appeal as a force multiplier and decision aid is clear given its potential for rapidly executing time-consuming, mundane, or even dangerous tasks. However, discussion of future AI applications can be vague or overly optimistic given limited technological understanding and non-linear trends in AI advancement.[8] Given these misunderstandings, using the OODA loop to frame discussions about military AI applications may stretch the OODA concept beyond its useful limitations and over-emphasize speed at the cost of other key metrics, like decision quality and human-machine team performance.

First, from a conceptual standpoint, phrases like 'hacking' or 'outpacing' the adversary's OODA loop may inaccurately imply that the adversary's decision-making calculus mirrors our own. In the context of using AI to outpace the enemy, strategic-level decision-makers could inappropriately assume symmetric thinking, access to information, or understanding of a specific situation.[9] While the OODA framing aims to convey the importance of superior decision speed, it is important to consider how adversaries' decision-making might differ from one's own, both for exploitative advantages and introspective vulnerability analysis.

Second, focusing purely on speed could miss the importance of decision quality and attention to timing. AI-enabled decision-making would ideally not only happen faster than the enemy's but would lead to effective action at the most advantageous moment relative to the adversary.[10] Quicker decisions are not necessarily better, and speeding through one's own OODA loop so quickly that it becomes disassociated from the adversary's may be less helpful than acting at the moment of most significant comparative advantage.

Third, it is not clear that the OODA loop scales to the strategic level or across operations, or even beyond its original one-on-one fighter context. When scaled-up to include multiple operators within their own, differently paced loops, Boyd's closed-loop system quickly becomes an open system-of-systems with dependent components. Vulnerable points increase with scale; as sub-systems span the tactical through strategic levels, their complexity dilutes the OODA model's usefulness.[11] Intelligence, Surveillance, and Reconnaissance (ISR) integrity is a risk in any military decision-making process given imperfect information; however, emphasizing rapid action could increase the negative effects of compromised observation and orientation on strategic decisions and effective outcomes. The OODA loop's centralized structure may also be unrealistic strategically given command structures and devolved authorities. AI could cut across the fog and friction of war, but AI-enabled strategic thinking should not be limited by the OODA framework.

Technological Challenges

In addition to the conceptual limitations of AI speeding the OODA loop, existing technological challenges should give the framework's proponents pause. Potential future applications of AI to military decision-making are manifold; image recognition is broadly applicable across ISR, predictive analytics can help with maintenance and route planning, web trawlers can collect valuable open-source information, and AI-enabled sensing could give warfighters increased situational awareness. But today's AI capabilities carry common risks that may make emphasizing speed as a key performance metric less desirable.

AI's ability to recognize images (observe) outside of certain conditions is highly limited and does interpret their function based on form (orient). Difficulty training algorithms stemming from inadequate data also poses risks to correctly observing and orienting, such as model overfitting or underfitting, and cultivating training data itself introduces the possibility for unintentional bias.[12] At present, black box characteristics of deep learning systems hamper explaining their choices and testing and evaluating for potential emergent behaviours.[13] These challenges to human understanding lessen the likelihood of quicker decisions and rapid positive effects in human-machine teams.

AI-enabled big data tools, particularly as aids for non-warfighting functions and decisions where representative data exists as with systems maintenance, may offer the best near-term prospects for military AI application. Yet even then, such tools require massive amounts of specific information to produce analysis that is not over-generalized to the data set. In some cases, these analysis tools could increase access to information that ultimately possesses little value to decision-makers and demands further human judgment to wade through, increasing cognitive load and creating additional human-machine teaming challenges.

Even assuming AI technologies function perfectly in the future, nearing machine decision cycle speeds may not be a good thing. Technology will not always plug neatly into human processes and may require humans to adapt in order to avoid automation bias, defaulting to reliance on machines.[14] Contested environments may create incomplete situational awareness even with superior observation tools, leading decision-makers without sufficient understanding of technological limitations toward poor choices. Furthermore, AI could lead to unintended escalation. A 2020 RAND wargame found that 'widespread AI and autonomous systems could lead to inadvertent escalation and crisis instability,' with machine decision-making speeds leading to quicker escalation and weakening deterrence. Machines in that wargame also struggled to respond to de-escalatory signals as humans might.[15] Add uncertainty over the impact of AI's potential to affect nuclear deterrence, and the risks of speedy AI begin to mount.[16] That is even before weighing unresolved legal, moral, and ethical concerns about using AI and AI-enhanced autonomy for combat. For example, international bodies and individual states have emphasized meaningful human control or appropriate levels of human judgment for AI-enabled capabilities such that potential liability for system malfunctions like targeting errors remains with a human.

Implications for Militaries

The limitations of the OODA-AI framing expose how important it is for operators and decision-makers to firmly grasp the strengths and limitations of AI and other emerging technologies. Military leaders need to be well-enough versed in the particulars of AI to recognize the realistic extent of its tactical, operational, and strategic value beyond simply accelerating decisions. Focusing on speed as a key metric is insufficient. New problem sets posed by adversaries in traditional domains already challenge officers well-schooled in doctrine, strategy, and warfighting. Incorporating algorithmic tools that perform best in constrained contexts does not guarantee near-term success.

Militaries should weigh how to use AI creatively in the context of competition. Effective AI is highly dependent on input quality, and future contested environments where adversaries deny or poison information may not be the best initial settings to deploy AI tools. How can militaries use AI for non-combat functions that exploit comparative advantages over adversaries? How can AI solve problems in constrained contexts, such as logistics, base functions, or personnel policies? What safeguards are necessary to protect against mistakes by non-technical users and to cultivate comparative human judgment advantages?

Even as AI advances, warfare will remain human-centric. Educating operators and decision-makers about the military implications of emerging technologies and establishing a core of common understanding with allies should help adapt tech-enabled decision-making for future warfighting. If AI-enabled technologies create scenarios where human values and input are necessary, operators at all levels need basic fluency in these systems' capabilities to properly use them and trust their effective functioning. Because humans will remain the most important cogs in the decision cycle for the foreseeable future, effectively integrating human judgment and machine function with AI will become either a source of military competitive advantage – or a liability.[17]

Creative, aspirational thinking about future applications of military AI is important; to borrow a phrase, the new wine of potentially revolutionary technology should not be put in old conceptual bottles.

Mr Owen J. Daniels is a research associate in the Joint Advanced Warfighting Division at the Institute for Defense Analyses in Alexandria, Virginia. He previously worked in the Scowcroft Center for Strategy and Security at the Atlantic Council and at Aviation Week magazine, and leads Young Professionals in Foreign Policy's Fellowship Program.

Endnotes

1. Gross, George. M., 'Nonlinearity and the Arc of Warfighting', Marine Corps Gazette (2019): p. WE44-47, https://mca-marines.org/wp-content/uploads/Nonlinearity-and-the-Arc-of-Warfighting.pdf, accessed 26 Mar. 2021.
2. Trautman, Erik, 'How Artificial Intelligence is Closing the Loop with Better Predictions', Hackernoon, 26 Jul. 2018, https://medium.com/hackernoon/how-artificial-intelligence-is-closing-the-loop-with-better-predictions-1e8b50df3655, accessed 26 Mar. 2021; Blondeau, Antoine, 'What Do AI and Fighter Pilots Have to Do with E-Commerce? Sentient's Antoine Blondeau Explains.' 5 Dec. 2016, https://www.ge.com/news/reports/ai-fighter-pilots-e-commerce-sentients-antoine-blondeau-explains, accessed 26 Mar. 2021.
3. Strickland, Frank, 'Back to basics: How this mindset shapes AI decision-making', Defense Systems, 30 Sep. 2019, https://defensesystems.com/articles/2019/09/18/deloitte-ai-ooda-loop-oped.aspx, accessed 26 Mar. 2021.
4. Freedberg, Jr., Sydney, 'JAIC Chief Asks: Can AI Prevent Another 1914?', Breaking Defense, 11 Nov. 2020, https://breakingdefense.com/2020/11/jaic-chief-asks-can-ai-prevent-another-1914/, accessed 26 Mar. 2021.
5. Hitchens, Theresa, 'Exclusive: J6 Says JADC2 Is A Strategy; Service Posture Reviews Coming', Breaking Defense, 4 Jan. 2021, https://breakingdefense.com/2021/01/exclusive-j6-says-jadc2-is-a-strategy-service-posture-reviews-coming/, accessed 26 Mar. 2021.
6. Goldfarb, A. and Lindsay, J., 'Artificial Intelligence in War: Human Judgment as an Organizational Strength and a Strategic Liability', Brookings Institution, 2020, https://www.brookings.edu/wp-content/uploads/2020/11/fp_20201130_artificial_intelligence_in_war.pdf, accessed 26 Mar. 2021.
7. Anderson, W., Husain, A., and Rosner, M., 'The OODA Loop: Why Timing is Everything', Cognitive Times (Dec. 2017), p. 28–29, https://www.europarl.europa.eu/cmsdata/155280/WendyRAnderson_CognitiveTimes_OODA%20LoopArticle.pdf, accessed 26 Mar. 2021.
8. Richbourg, Robert, 'It's Either A Panda Or A Gibbon: AI Winters And The Limits Of Deep Learning', War on the Rocks, 10 May 2018, https://warontherocks.com/2018/05/its-either-a-panda-or-a-gibbon-ai-winters-and-the-limits-of-deep-learning/, accessed 26 Mar. 2021.
9. Pietrucha, Mike, 'Living with Fog and Friction: The Fallacy of Information Superiority', War on the Rocks, 7 Jan. 2016, https://warontherocks.com/2016/01/living-with-fog-and-friction-the-fallacy-of-information-superiority/, accessed 26 Mar. 2021.
10. Luft, Alastair, 'The OODA Loop and the Half-Beat', In The Strategy Bridge, 17 Mar. 2020. https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat, accessed 26 Mar. 2021.
11. Ibid. 9.

12. Ramzai, Juhi, ‘Holy Grail for Bias-Variance Tradeoff, Overfitting & Underfitting’, towards data science, 12 Feb. 2019, https://towardsdatascience.com/holy-grail-for-bias-variance-tradeoff-overfitting-underfitting-7fad64ab5d76, accessed 26 Mar. 2021.
13. MathWorks®, ‘What is Deep Learning? How it Works, Techniques, and Applications’, https://www.mathworks.com/discovery/deep-learning.html, accessed 26 Mar. 2021.
14. Oakden-Rayner, Luke. ‘Medical AI Safety: Doing it wrong’, Jan. 2019, https://lukeoakdenrayner.wordpress.com/2019/01/21/medical-ai-safety-doing-it-wrong/, accessed 26 Mar. 2021.
15. Wong, Y. H., Yurchak, J., Button, R., Frank, A., Laird, B., Osoba, O., Steeb, R., Harris, B., Joon Bae, S., ‘Deterrence in the Age of Thinking Machines’, Santa Monica: RAND Corporation, 2020, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf, accessed 26 Mar. 2021.
16. Loss, R. and Johnson, J., ‘Will Artificial Intelligence Imperil Nuclear Deterrence?’ War on the Rocks, 19 Sep. 2019, https://warontherocks.com/2019/09/will-artificial-intelligence-imperil-nuclear-deterrence/, accessed 26 Mar. 2021.
17. Ibid. 6.

Policy and Strategy

Dynamic C2 Synchronized Across Domains

Superiority in the Electromagnetic Spectrum

NATO Space

© Maxim Evdokimov/Shutterstock.com

Cyberspace and Joint Air and Space Power

XVII

Any Speed; Always Relevant

By Lt Col Paul J. MacKenzie, CA Air Force
Joint Air Power Competence Centre

Introduction

When examining the Cyberspace Domain where the projection of Air and Space power is concerned, it is just as relevant for mission success to maximize the defence of systems and information throughout the slow and arduous process of aerospace project delivery, as it is during the rapid and time-sensitive coordination and execution of Air and Space operations. This paper will outline the relevance of considering Cyberspace, and cybersecurity in particular, from the earliest slow-moving stages of Air and Space systems Research and Development (R&D), and how activities in these phases can eventually influence the Air and Space power capability gaps with potential adversaries. The paper will also discuss the importance of a secure and reliable cyber-network through to the opposite end of the Air and Space power spectrum, from mission planning and the publication and distribution of orders, to the fast-paced execution and coordination of Air and Space operations to deliver Air and Space power with precise timing and accuracy.

Research and Development

Considering the earliest stages of Air and Space Power capability delivery, with modern systems inextricably dependent on the information technology, operating systems, and applications that comprise the physical and logical layers of the Cyberspace domain, aerospace systems are vulnerable to exploitation from adversaries. The vulnerabilities are present from the early stages of R&D through to when systems are delivered. Adversaries will find or create and exploit vulnerabilities throughout the slow and laborious program delivery period in order to reduce the capability gap, exploiting the weakness in cyber defences to impede the effectiveness of NATO forces while working to improve that of their own. Industrial espionage of military programs via Cyberspace has been stated to be part of what represents one of the largest transitions of wealth in human history.[1] China, for example, is reported to have stolen, and continues to steal, data on US stealth fighters, engines, radars and missiles.[2] This data will have been leveraged to influence improvements in the design, production, and performance of their systems and assist in their reconnaissance (and possibly exploitation) of vulnerabilities in allied systems. The 2020 attack on the SolarWinds business software,[3] impacting thousands of government, public, and private organizations globally, is recent evidence of the ongoing vulnerability and threat to industry and, inevitably, the military which relies upon it.[4]

Strategic Planning to Mission Execution

The shrinking capability gap and loss of advantage presents many challenges as this impacts strategy and mission planning, influences decisions regarding orders of battle, risk assessment, estimating potential success rates and many other factors for Air and Space operations. Considering the actual execution of Air and Space operations, the integration and coordination of resources of multiple domains in time and space is essential for mission success, so securing the cyber-network across which this coordination takes place is paramount. As all nations enhance their capabilities, Cyberspace is an increasingly contested environment. Achieving supremacy in Cyberspace in this era, against a peer or near-peer adversary, is unlikely; superiority is more achievable. Still, claiming only superiority recognizes that the enemy has a vote and can influence the Cyberspace domain to some degree. What is critical to understand is that, in modern operations, freedom of manoeuvre in Cyberspace will be challenged, so superiority is not permanent but temporary. This is extremely relevant when Air and Space capabilities, as well as those in other domains, in multi- or all-domain operations, are integrated with Cyberspace and brought to bear against an adversary. In such operations, mission success hinges on the skilful coordination and management of resources and on the availability of systems, in and through Cyberspace, being assured. This integration is exemplified by recent engagements coordinated by Combat Controllers (CCT) during operations in Afghanistan. The CCTs employed a variety of communications (PRC 177F and MBITR Radios),[5] to communicate with multiple aircraft (F-18 Fighter/Bombers, AC-130 Gun Ships, E3 Airborne Warning and Control [AWACS], E-8 JSTARS, P-3 Orions, Predator UAS, AH 64 Apache Attack and CH 47 Chinook Transport Helicopters) and multi-service special operations forces on the ground (Navy Seals, Rangers, Delta Force operators, Air CCTs). They coordinated flying and ground movement, managing airspace using several systems (Falcon View digital mapping, deployable navigational beacons, portable Global Positioning System (GPS)) while directing a variety of ordnance (Blu-118/B 2000n thermobaric laser-guided bombs, JDAMS) for precise and overwhelming effect.[6, 7] All of these systems, when digitally interconnected to establish a larger system, lethal as it was, had myriad attack surfaces with varying degrees of vulnerability to attack in and through Cyberspace, which introduced greater risk to the mission. Fortunately, at the time these missions were executed, with this arrangement of forward command and control, Allies enjoyed at least superiority, if not supremacy, over the enemy in Cyberspace. Consequently, the aggregate results were achieved with optimum speed and relevance with respect to delivery of Air and Space power. Historically speaking, the combination resulted in 'one of the deadliest and least known forces in the history of human warfare.'[8] The degree of success realized in these missions, however, hinged on the confidentiality, availability, and integrity of information and the systems operating in real-time in the Cyberspace domain, a condition that will be challenged in the future by potential peer and near-peer adversaries.

Defence

The defence and resilience of the Cyberspace domain is critical to mission success. NATO relies on the NATO Communications and Information Agency (NCIA) to defend its own Cyberspace links and nodes. Contributing nations have agreed, through the Cyber Defence Pledge, to ensure the resources they force generate for NATO have been provided sufficient cybersecurity.[9] Honouring this pledge requires each nation to implement programs to provide the maximum level of security. For example, the United States is implementing a Zero Trust Architecture (ZTA)[10] for Federal Agencies to enhance security and has adopted the Cybersecurity Maturity Model Certification as part of multiple lines of effort focused on the security and resiliency of their Defense Industrial Base in order to enhance the protection of the supply chain.[11]

It is vital that Cybersecurity be achieved to the greatest extent possible, though it is understood that it is impossible to protect systems completely. In the course of Air and Space operations, 'system components vary in importance to a mission, and this importance can change throughout the life of a mission'.[12] Consequently, 'these systems' risks to the Air mission from Cyberspace need to be identified, managed, and monitored throughout the life of the mission.'[13] Despite the very best efforts, systems may be degraded by adversary action in and through Cyberspace. Therefore 'the Air domain might need to carry out critical mission activities using vulnerable parts of Cyberspace simply because it has no alternative.'[14] Indeed, the 2017 Annual Report of the US Director, Operational Test and Evaluation (DOT&E) highlighted that 'although directed by The Chairman of the Joint Chiefs of Staff in 2011 and endorsed by two subsequent Secretaries of Defense, DOT&E has not observed many demonstrations that Commands can 'fight through' a major cyber-attack and sustain their critical missions.'[15] On the degree of difficulty scale of measures to adapt to cybersecurity threats, exercising in a degraded environment should be considered easier relative to most measures and be high on the list of priorities, particularly when considering the possible consequences of being unprepared.

Offense

NATO, as a defensive Alliance, does not possess offensive Cyberspace capabilities of its own. However, this does not preclude a commander from exploiting offensive capabilities when offered voluntarily by Allies. Still, coordinating offensive Cyberspace operations so they are executed at the speed of relevance particularly when in concert with other components in Joint All Domain Operations is a highly complex endeavour. 'The timing and sequencing of joint operations has always presented unique challenges, cyber adds a new dimension.'[16] In reality, it takes a great deal of time to plan and progress through the steps necessary to produce effects in/through Cyberspace, steps collectively referred to as the Cyber Kill Chain. Some attack surfaces and/or vulnerabilities that the planning would aim to exploit may have changed before the weapon is deployed, which means many possible vulnerabilities will need to be found, or even created, in order to increase the likelihood of success. That said, 'once a system is exploited, the effects of a cyber-attack can be nearly instantaneous.'[17] In such circumstances, where the success of a joint mission is dependent on the success of a Cyberspace operation, it would be necessary to design the payload with a trigger to coincide with the correct conditions to exist for allied conventional forces, such as a time, traffic pattern, or message content on an adversary's network.

Future

To be able to operate in the Cyberspace domain at the speed of relevance in the future NATO must successfully exploit emerging trends and technologies. Close cooperation is required between governments, industry, academia, and the military. From a defensive perspective, NATO's potential adversaries are automating their attacks, which means NATO must 'use the same kind of automation and artificial intelligence and machine learning to counter those attacks.'[18] This includes using AI 'to identify and mitigate zero-day cyber-attacks and advanced persistent threats.'[19] The same technologies will be leveraged, in a similar but opposite fashion, to identify and help create vulnerabilities for use in offensive Cyberspace operations. Advanced technologies are, according to the Chief Scientist for the US Government Accountability Office, 'a double edge sword'[20] the more we employ the more vulnerable we become. The objective is to optimize the advantages and reduce the disadvantages. AI and quantum computing, 'each of these is a massive, disruptive technology … (and) what makes each even more powerful is their convergence … These are linked by cyber; either as a core competency or in a vital supporting role.'[21] Further into the future are the possibilities of controlling technologies via brain-to-machine interfaces. The promise of this possibility has been made more realistic based on recent work with implants coated with a polymer that facilitates the interface between synthetic materials that have an electronic charge in solid-state, and biological tissue that has an ionic charge in a wet state.[22] Our ability to exploit this and similar advances in technology will help to increase the speed of transforming operational intent into effect.

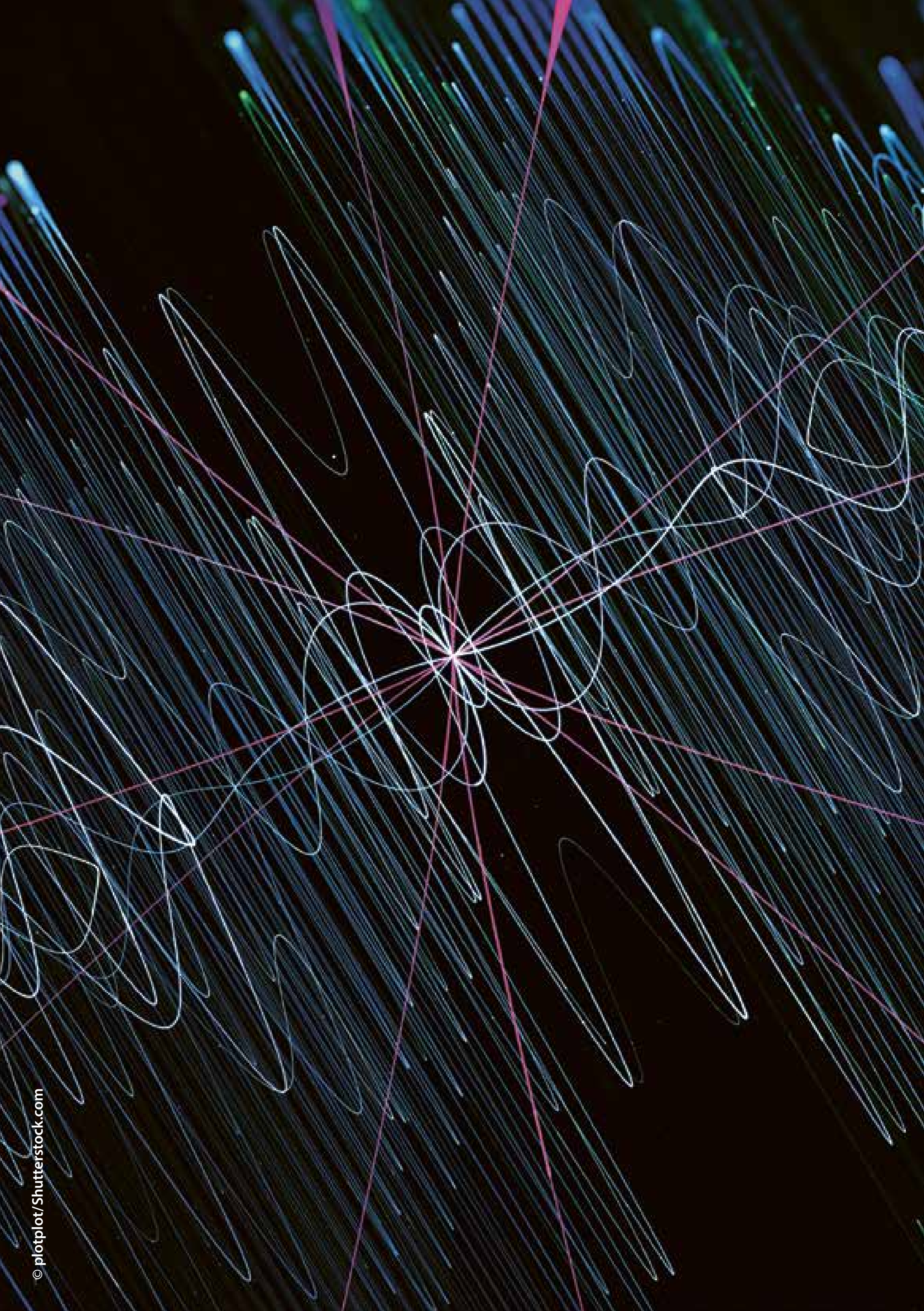
Conclusion

If NATO is to continue to achieve success, protecting systems and information from attacks in and through Cyberspace, while at the same time exploiting the advantages the domain provides, must be a core requirement going forward. Cyberspace must be at the forefront in consideration from the early stages in force development through to force generation and employment. As with all domains, it is imperative NATO outpace and out-innovate its potential adversaries if it is to reach the speed and operational tempo required to generate effects and achieve the technological advantage, if not outright superiority, necessary to be an effective military instrument of power at the speed relevance in the NATO warfighting concept.

Lieutenant Colonel Paul J. MacKenzie (CA Air Force) MSM (US), CD. A Communications and Electronics Engineering (Air) Officer in the Royal Canadian Air Force, he examines Cyberspace as it relates to NATO Joint Air and Space Power and from a defensive perspective through to the potential in exploiting offensive effects. He holds a Master's of Science degree in Computer and Information Technology (System Engineering), is a graduate of the Canadian Forces Joint Command and Staff Program and has over 32 years of experience in the provision of IT/CIS to operations.

Endnotes

1. Flannery, Russell, 'China Theft of U.S. Information, IP one of the Largest Wealth Transfers in History: FBI Chief' (published online 7 Jul. 2020), https://www.forbes.com/sites/russellflannery/ 2020/07/07/china-theft-of-us-information-ip-one-of-largest-wealth-transfers-in-history-fbi-chief/ ?sh=27b060834440, accessed 24 Jan. 2021.
2. Carlin, John, Dawn of the Code War, Public Affairs, 2018, p. 274–275.
3. Brewster, Thomas, 'DHS, DOJ and DOD Are All Customers of SolarWinds Orion, The Source of the Huge US Government Hack' (published online 14 Dec. 2020), https://www.forbes.com /sites/ thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/?sh=7785505d25e6, accessed 19 Jan. 2021.
4. The attack itself involved the use of a Trojan Horse on IT Monitoring and Management software, enabling creation of a back door and subsequently permitting lateral movement and data theft. The malware was sufficiently sophisticated to permit evasion from detection and to obscure its actions once it had successfully compromised the system by masquerading as a legitimate improvement program protocol.
5. Army Navy Portable Radio communications (AN/PRC) 117F: A multiband, man-portable, tactical, software-defined combat-net radio with embedded communications security, satellite communications, and electronic countermeasures. AN/PRC -148 Multiband Inter/Intra Team Radio (MBITR): A multiband, handheld, tactical, software-defined radio, widely used by NATO forces around the world.
6. Schilling, Dan, and Chapman Longfritz, Lori, 'Alone at Dawn – Medal of Honor Recipient John Chapman and the Untold Story of the World's Deadliest Operations Force', Hachette Book Group, Inc., 2019.
7. Naylor, S., Relentless Strike, The Secret History of Joint Special Operations Command, St. Martin's Press, 2015.
8. Ibid. 4., p. 9.
9. NATO, 'NATO Cyber Defence Pledge', 8 Jul. 2016, https://www.nato.int/cps/en/ <natohq/ official_texts_133177.htm, accessed 28 Jan. 2021.
10. Rose, S. W., Borchert, O., Mitchell, S., and Connelly, S., Zero Trust Architecture, NIST Special Publication 800-207, US Department of Commerce, 2020.
11. Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory, 'Cybersecurity Maturity Model Certification (CMMC)' Version 1.02, 18 Mar 2020.
12. Cummins, James, 'The Challenges of Cyber Freedom of Manoeuvre For Airpower in the Information Age', Joint Services Command and Staff College, (2020): p. 12.
13. Ibid. 10., p. 18.
14. Ibid. 10., p. 19.
15. US Director Operational Test and Evaluation, 'FY 2017 Annual Report', Jan. 2018, p. 319.
16. McArdle, Jennifer, 'Victory Over and Across Domains – Training for Tomorrow's Battlefields', Center for Strategic and Budgetary Assessments, 2019, p. 41.
17. Ibid. 14., p. 42.
18. Seffers, George I., 'DISA, JAIC Developing AI-Enabled Cybersecurity Tool – Automation is the key to keeping up with adversaries', SIGNAL, Dec. 2020, p. 16.
19. Ibid. 16., p. 17.
20. Ackerman, Robert K., 'A Cyber Thread Runs Through Government Future Assessments', SIGNAL, Oct. 2020, p. 31.
21. Ibid. 18.
22. Seffers, George I., 'The Brain-to-Machine Interface Just Became Better', SIGNAL, Dec. 2020, p. 38.



© plotplot/Shutterstock.com

Electronic Protective Measures

XVIII

It's About Protecting Access, Not Aircraft

By Mr Dirk A. D. Smith and
Mr Steve 'Tango' Tourangeau
Reginald Victor Jones Institute

While the world can argue about whether words can hurt, one thing is clear: misunderstanding words can kill, especially in the context of the military. In the world of electromagnetic warfare, just such a misunderstanding of the term 'Electronic Protective Measures' (EPM) has left NATO less prepared for the field of battle and has already caused soldiers to fall when and where they should not. This article addresses the confusion, clears up the definitions through examples of each, and makes the obvious suggestion of what needs to be done.

The Confusion

When most people think of EPM, they think about platform self-protection (such as jammers or chaff and flares), but that is incorrect. Jammers and the like are classified as Electronic Defence (ED). In contrast, EPM is about protecting our access to, and the ability to operate in, the electromagnetic spectrum, regardless of conditions (e.g., when access is contested, congested, or even denied). An example of EPM features would be the use of low probability of detection communication technology to hide our signals.[1]

This confusion is not new, but it is problematic. The conflation of EPM and ED, especially by people at remarkably high levels, results in the belief that EPM is automagically part of ED and, therefore, built into the systems that we have operating today … it is not. For example, the new Active Electronically Scanned Array (AESA)[2] antennas that replace parabolic dish antennas in US forces are wreaking havoc with US Radar Warning Receivers (RWR) operating nearby. The AESA works fine but its transmissions interfere with the RWR which does not have sufficient EPM features and results in the loss of situational awareness of the threat environment for the aircrew. In contrast, in aircraft with the traditional parabolic dish antenna that operated on specific frequencies, it was easy to blank out those frequencies on the RWR. With AESA and its much broader frequency range, it is very difficult to blank out those frequencies without making the RWR virtually useless.

A more graphic example of deployed systems that were not built with (or tested for) adequate EPM was described by Dave Tremper, Director of Electronic Warfare at the Office of the United States Secretary of Defense for Acquisition and Sustainment, when speaking as a panellist in a January 2021 webinar hosted by the Potomac Officers Club[3]: 'CREW, a radio-controlled IED jammer, puts out energy across the spectrum which is intended to stop IEDs from being communicated with.[4] CREW can overlap with the way that we communicate, so we had to turn one on and turn one-off to keep moving and that has resulted in some pretty awful scenarios that are unclassified.' Tremper went on to describe not just what could be, but what in general terms has occurred: 'There is the warfighter who's in the convoy who gets pinned up against the guard rail which is a prime IED location. He's got his CREW jammer going but he can't talk because his radio isn't working when his CREW jammer is on so you've got this scenario in which you can either talk and try to get help and turn your jammer off and risk the chance that this IED is going to explode or you can keep your jammer on and attempt to fight your way out. It becomes this life-or-death situation and that is completely unacceptable.' And that is what happened during numerous operations: CREW was operating, jamming as designed. However, when members of the various convoys needed to communicate, CREW was shut down, IEDs went off, and soldiers died.

Michael Ryan[5], then Deputy Project Manager for Electronic Warfare in the Program Executive Office for Intelligence, Electronic Warfare and Sensors (PEO IEWS), stated in a 2013 SIGNAL Magazine article that the Army is rife with documented cases where a soldier had to choose between protection from an active jammer or turning off the jammer to communicate and some of these forced decisions led to loss of life.[6]

Clearing Up Definitions

Before clarifying EPM versus ED, one other item of lexicon house-cleaning is needed. Generations of warfighters who jammed enemy radar or communications were known commonly as electronic warfare soldiers. Now that is changing to electromagnetic. The term electronic refers to the control of electric current by various devices[7] while electromagnetic refers to electromagnetic waves.[8] Therefore, while electronic refers to computers and myriad other devices, electromagnetic narrows the focus to waves and the use of same throughout the electromagnetic spectrum. While both terms are still commonly used, the change is embedded in US Air Force doctrine, such as in the 'Introduction to Electromagnetic Warfare', published by the Curtis E. Lemay Center for Doctrine Development and Education.[9] With respect to EPM and ED, and because the differences can seem rather gray at first, it is helpful to envision hard examples. Thus, consider the following two examples of ED, followed by two examples of EPM:

What Electronic Protective Measures are NOT

In contrast to EPM, ED systems are stand-alone systems that include features like jamming to confuse enemy detection and communication and decoys that steer incoming missiles away.

- **Jamming:** The AN/ALQ-131 Electronic Countermeasures (ECM) pod is a good example of a system with ED features, protecting both aircrews and aircraft since the 1990s. To date, and with periodic upgrades, more than 1,600 produced by Northrup Grumman have been deployed with recent variants found on the F-16 Block 60 and F-35 Joint Strike Fighter. The ALQ-131's ED features are enabled by responding against radar threats with repeater or transponder electronic jamming techniques. Weighing in at 600 pounds (270 kilogram), it has a modular design for multiple frequency band capability and can be quickly reprogramed against changing threats.[10]
- **Decoying:** The MK 53 DLS Nulka system is an Australian-designed and developed active missile decoy built by an Australian/American collaboration. It is a rocket-propelled, disposable, offboard, active decoy designed to seduce anti-ship missiles away from their targets. It has a unique design in that it hovers in mid-air while seducing the incoming anti-ship missile.

  Specifically, the MK 53 DLS system is fitted to the Canberra Class amphibious assault ships, Adelaide Class and Anzac Class frigates, and the new Hobart Class guided-missile destroyers.[11] It is also used on more than 122 US ships.[12] The word 'Nulka' is the Australian Aboriginal language meaning 'be quick,' which apparently it is.

What Electronic Protective Measures ARE

EPM are a way for systems to function within the spectrum no matter the conditions including contested, congested, denied access, etc. It is also important to note that electromagnetic protection is not a platform or system. Rather, EPM are the features included in spectrum-dependent systems. That's it. Examples of EPM features include Low Probability of Interception/Low Probability of Detection (LPI/LPD), anti-jam, frequency hopping, and stealth.

- **Low Probability of Interception/Detection:** Radar often must contend with radar threats such as Electronic Attack (EA) systems and Anti-Radiation Missiles (ARM); systems designed to interfere with or degrade radar effectiveness or even destroy the radars themselves. Radar systems equipped with LPI/LPD features make radar signals less subject to interception and detection. Put another way, LPI/LPD is the ability to 'see and not be seen'.[13]

  Aytug Denk, author of a well-known thesis on the detection and jamming of LPI radar, stated that 'to survive these countermeasures and accomplish their missions, radars have to hide their emissions from hostile receivers. For this purpose, and to mask their presence, radars use power management, wide operational bandwidth, frequency agility, antenna side lobe reduction, and advanced scan patterns (modulations).'[14] This, then, is a good example of EPM because the features are designed to protect access to and use of the spectrum when faced with adversary attempts to prevent such use. An example of LPI Radar (LPIR) includes the Northrop Grumman AN/APG-77 deployed on the F-22 Raptor. Known as multi-mode tactical radar, this enables the pilot to track and shoot at multiple threat aircraft before the adversary's radar even detects the Raptor.
- **Frequency hopping:** While radio communications help Command and control (C2) of the battlefield, the transmissions can also be picked up by adversaries effectively eliminating the C2 advantage (or transferring that advantage to the adversary). One way to combat this risk is through the use of Software-Defined Radios (SDR) that enable different EPM features such as automated frequency hopping.

> An SDR is '… a radio in which the properties of carrier frequency, signal bandwidth, modulation, and network access are defined by software. Modern SDR also implements any necessary cryptography, forward error correction coding, and source coding of voice, video, or data in software as well.'[15]
>
> Another benefit of SDR is the ability to execute over-the-air or other remote reprogramming, allowing 'bug fixes' to occur while a radio is in service, thus reducing the time and costs associated with operation and maintenance.[16] Consider the difference with hardware-based radios which would require getting it to base, opening the system up, and replacing parts while the SDR system could be updated (repaired) while in use far afield (or airborne).

To sum it all up, EPM create the ability to defeat EA.

What Do We Do Next?

With the confusing conflation of EPM and ED that has sadly resulted in the deployment of systems with insufficient EPM that has in turn resulted in unnecessary deaths, we are now left with the question of how to resolve it. The first step is to simply understand this issue which is the intent of this article. That still leaves us with another most crucial step: Formal requirements that mandate full and proper EPM features as part of the development, production, testing and deployment of all electromagnetic spectrum-reliant systems. So, while it is true that misunderstanding words can kill, perhaps the words in this article will help reduce what Tremper called 'completely unacceptable'.

Mr Dirk A. D. Smith is Director of Research for the Reginald Victor Jones Institute (RVJ Institute) Center for Excellence in Electromagnetic Spectrum Operations and is an international award-winning technical writer and freelance journalist. He specializes in the research, analysis, writing and presentation/publishing of complex technical knowledge. This work often includes interviewing Subject Matter Experts (SME) for internal and external corporate, military, and intelligence communications.

Mr Steve 'Tango' Tourangeau is the Vice President and Chief Operating Officer of Warrior Support Solutions, LLC as well as Co-Founder and Dean of the Reginald Victor Jones Institute (RVJ Institute) Center for Excellence in Electromagnetic Spectrum Operations. He provides expertise for the DoD, industry and academia to advance Electromagnetic Spectrum capabilities. Tango is a retired Air Force officer with over 1,500 hours as Flight Test Navigator and Electronic Warfare Officer.

Endnotes

1. 'Low Probability of Detection Communication: Opportunities and Challenges', IEEE Wireless Communications, Volume: 26, Issue: 5, Oct. 2019 (published online 25 Oct. 2019), https://ieeexplore.ieee.org/document/8883125, accessed 26 Mar. 2021.
2. https://military.wikia.org/wiki/Active_electronically_scanned_array, accessed 26 Mar. 2021.
3. https://potomacofficersclub.com/events/poc-achieving-spectrum-dominance-in-the-digital-battlespace/, accessed 26 Mar. 2021.
4. Van Pool, J. Elise, 'CREW: helping defeat IEDs', US Army, https://www.army.mil/article/67963/crew_helping_defeat_ieds#:~:text=CREW%20systems%20are%20helping%20Soldiers,to%20detonate%20the%20devices%20remotely.&text=CREW%20has%20been%20highly%20effective,by%20cell%20phones%20said%20Bowers, accessed 26 Mar. 2021.
5. LinkedIn profile Michael Ryan: https://www.linkedin.com/in/michael-ryan-0223/, accessed 26 Mar. 2021.
6. Ackermann, Robert K., 'Consolidation Is the Course for Army Electronic Warfare', SIGNAL Magazine, 1 Apr. 2013, https://www.afcea.org/content/consolidation-%E2%80%A8the-course-army-%E2%80%A8electronic-warfare, accessed 26 Mar. 2021.
7. Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/electronic, accessed 26 Mar. 2021.
8. Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/electromagnetic, accessed 26 Mar. 2021.
9. Curtis E. Lemay Center, 'Air Force Doctrine Publication (AFDP) 3-51, Introduction to Electromagnetic Warfare', https://www.doctrine.af.mil/Portals/61/documents/Annex_3-51/3-51-D03-EW-EW-Introduction.pdf, accessed 26 Mar. 2021.
10. National Museum of the USAF, ALQ-131 ECM Pod (published online 29 May 2015) https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/197590/alq-131-ecm-pod/, accessed 26 Mar. 2021.
11. Royal Australian Navy, Nulka active missile decoy, https://www.navy.gov.au/weapon/nulka-active-missile-decoy, accessed 26 Mar. 2021.
12. US Navy, Naval Sea Systems Command, MK 53—Decoy Launching System (Nulka) (last updated 16 Jan. 2019), https://www.navy.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=1&ModuleId=724&Article=2167877, accessed 26 Mar. 2021.
13. Fuller, K. L., 'To see and not be seen', IEE Proceedings F 137 (1): p. 1–9, https://digital-library.theiet.org/content/journals/10.1049/ip-f-2.1990.0001, accessed 26 Mar. 2021.
14. Denk, Aytug, Naval Postgraduate School, Monterey, California, Thesis: 'Detection and Jamming low probability of intercept (LPI) Radars' (published 2006), https://apps.dtic.mil/dtic/tr/fulltext/u2/a456960.pdf, accessed 26 Mar. 2021.
15. Fette, Bruce A., 'History and Background of Cognitive Radio Technology' (published online 2009), https://www.sciencedirect.com/topics/engineering/software-defined-radio#:~:text=A%20software%20defined%20radio%20is,data%20in%20software%20as%20well., accessed 26 Mar. 2021.
16. Wirelessnavigation.org, 'Software Defined Radio', https://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf, accessed 26 Mar. 2021.

© Matt Antonino/Shutterstock.com

Managing the Electromagnetic Spectrum

XIX

A Large-Scale Collective Action Problem for the 21st Century

By Mrs Melinda Tourangeau
Reginald Victor Jones Institute

'Effectively, change is almost impossible without industry-wide collaboration, cooperation, and consensus.'

Simon Mainwaring

This year's JAPCC conference theme asks the community to address the issues of Synchronization, Human in the Loop, Harmonization, and Resilience. Each of these issues share a common, yet invisible, feature: 100 % dependence on access to the Electromagnetic Spectrum (EMS). The NATO community is prudently looking at technologies, capabilities, investments, and Tactics, Techniques, and Procedures (TTP's) to ameliorate these issues. However, the very canvas that hosts all these activities remains in the shadows, ever invisible to the human eye. Perhaps that is why it has been so systemically overlooked. The EMS is there, though, and it plays a vital role in NATO's military operations. NATO must begin to look at the EMS holistically if it is going to remain relevant in the great power competition. This paper seeks to highlight the most compelling reasons why the EMS must be prioritized and brought into proper focus for NATO to be successful on the modern battlefield.

NATO's dependence on the EMS[1] goes far beyond the four issues called out in the JAPCC 2021 Call for Papers. It is safe to say nearly all military operations being planned today are 100 % dependent on access to the spectrum. And yet, ensuring that access is not being adequately addressed. Where are the Electronic Protective Measures (EPM)[2] taken on all EMS-dependent systems and the policies to drive those measures? Denial of Spectrum Denial[3] would seem to be in play ('What do you mean I won't have access to the spectrum? The lightning bolts are right there on my OV-1.').

Peer and near-peer adversaries have been watching NATO operate for the last twenty-five years with virtually uncontested access to the EMS. They have been planning to deny NATO forces this precious access and they know it is our proverbial Achilles Heel.[4] They have designed myriad systems to deny NATO access to the EMS and have already achieved some rewards. Russia took over the Ukrainian province of Crimea decisively; they employed Information Operations, controlled the civilian population's access to the EMS (i.e., Information Warfare), and rolled into that country with minimal kinetic actions or activity.

NATO has reared nearly two decades' worth of warfighters who have not experienced large-scale EMS denial. This situation naturally, but unfortunately, stems from the retired Cold War culture of awareness that the EMS is a bona fide target that can and will be denied. Even the IED fratricide episodes in the early and mid-2000s are fading into the rear-view mirror. This means that a large portion of the fighting force lacks an appreciation for, awareness of, and respect for operating in the EMS.

Finally, whether anyone realizes it now or not, the EMS is on its way to becoming a global public goods resource like clean water, safe food sources, and responsible industrial waste management.[5] A feature of a public goods resource is that it must be made available for everyone on the planet. Here's why the EMS qualifies: By 2030, there will be 5 billion users of the EMS and each user will have an average of 10 devices.[6] With this omnipresent mantle of the Internet of Things, there will arise a social obligation to give every human being access to the EMS (right now, access to the EMS is reserved for those who pay for it). With this much demand, the current static allocation practice of owning frequencies will not render enough capacity to accommodate that demand. This means the EMS will become an unrenewable sustainable resource in the very near future.[7] All of these issues point to a need for NATO to begin addressing the EMS holistically if it is going to be prepared for the future, both militarily and sociologically.

The confluence of disparate issues across a singular public good presents what is classically called a Large-Scale Collective Action Problem (L-SCAP).[8] A future where all users can use the EMS as they wish lies in treating the EMS as an L-SCAP.

Large-Scale Collective Action Problems

L-SCAPs have been studied heavily in the social sciences. In fact, there is a Centre of Excellence at the University of Gothenburg called, 'Centre for Collective Action Research (CeCAR[9])', which was stood up specifically to address the myriad issues that come with solving L-SCAPs. One main empirical finding from CeCAR's research is that the larger the problem, the more imminent the need to establish a neutral, third party to help solve it. If NATO were to set up such a third party, it could navigate these social challenges while simultaneously researching what is needed to maintain control of the EMS.

L-SCAPs are characterized by four conditions:

1. A large number of anonymous users–the current EMS users are virtually completely anonymous to one another, both in their identity and their various methods of using the spectrum.
2. Spatial distance–billions of EMS users are scattered across the globe.
3. Temporal displacement–the condition that outcomes and consequences of decisions we make today will not be made known for years to come.
4. Complexity–operating in the EMS presents NATO and our world with some of the most complex problems that modern civilization has ever faced.

In addition to these four explicit conditions, there are several underlying challenges with the EMS as an L-SCAP that make tackling the problem even more challenging.

Conflicting Interests

Users involved in an L-SCAP scenario organically want to maximize their expected benefit. In the EMS, it is undeniably true that all users, regardless of origin, want unfettered and ubiquitous access 100 % of the time. But users want this outcome for themselves at the expense of the greater good. This natural human penchant motivates users to 'want what they want when they want it,' so much so that they will all defiantly 'sit in the same boat',[10] risking its seaworthiness, not caring if they all go down with the ship. In other words, people will risk losing their joint resource unless they start cooperating. There is currently no incentive for the billions of anonymous users, their commercial/industrial overlords, and the world's military powers to join together to look at the EMS holistically. The large number of anonymous users makes it difficult to see that the 'Collective' would be better off if they begin to cooperate now.

Pareto Inefficiency

There is an economic consequence called Pareto Inefficiency inherent in L-SCAPs. An organization is said to be Pareto Efficient when its resources have been maximized such that any additional investment in products would result in a reduction in services, or any additional investment in services would result in a reduction in products. Organizations are able to operate on this curve when the responsibility, authority, and ownership of the process falls under one umbrella. L-SCAPs are perceived as being Pareto Inefficient because responsibility and authority rests among many powerful players. If any one player were to invest in standing-up a global EMS authority, because of a social norm known as free-riding[11], they would run the risk of being left to do it by themselves. This is why no entity has stood up yet, not even the US's Department of Defense (DoD). In the case of ubiquitous management of the EMS, responsibility is spread across the DoD, NATO Allied governments, the civilian telecom industry, the power industry, and the cybersecurity industry. This situation presents a palpable barrier for any single existing authority to stand-up and take charge of the problem.

Technological Innovation

Pockets of innovation and technology alone, even the most compelling advances in capabilities, will not do the trick nor will they do it in the time frame needed. If a future of effective EMS utilization is to be realized, autonomous dynamic EMS access schemes will need to be designed and built into every EMS-dependent system. Even if, and when, scientific efforts in artificial intelligence and machine learning come to maturity and enable autonomous dynamic EMS access capabilities, there is still the matter of EMS allocation priorities and schema that need to be discussed, vetted, adopted, ratified, and then disseminated to NATO countries. This challenge falls solely into the sociological realm of discussion, collaboration, negotiation, mediation, and compromise. To add to the challenge, these conversations must occur among disparate user groups. No advanced technological system or strategy is going to ameliorate that.

Pockets of Cooperation

Perhaps NATO is hoping that pockets of cooperation will naturally emerge to navigate the challenges associated with operating in the EMS. However, there is a latent barrier to spontaneous cooperation among users associated with a L-SCAP:[12] anonymity (mentioned previously). This introduces inherent stressors that have been shown to prohibit spontaneous cooperation.[13] In 1740, David Hume proclaimed in his work, A Treatise of Human Nature, 'Although two neighbours agree, … a thousand neighbours becomes a matter too complex to execute.'

The Information Superhighway

Managing the EMS holistically is going to require a significant culture change. Users are scattered so far and wide across the globe, using the EMS in so many different ways and residing in so many different pockets of industrial, municipal, communal, and military operation that they do not share a common understanding or belief system for using the EMS. To bring this point home, let's consider the basic vehicle driver. There are countless numbers of them, and they all share the road peacefully. They are able to do this because every driver has an understanding of three things: a recognized set of rules, basic knowledge of how their vehicles work, and respect for one another's use of the same highways. The Information Superhighway, heavily dependent upon the EMS, will need its users to possess similar qualities. Without a fundamental culture of understanding, awareness, respect and compliance, a future of peaceful coexistence is out of reach for operating in the EMS.

Summary

In order to address the more socially charged and very specific issue of EMS management that is an integral part of 21st century military operations, it would behove NATO to consider establishing a neutral third party to investigate the social as well as technological challenges associated with managing the EMS. Such an entity could establish a set of standards, similar to the aforementioned driving laws, that work for the entire community, be they from defence, commercial, municipal, or other operating groups.

Technology, capabilities, and strategy alone will not solve the issues coming in the EMS. NATO's mission should include a focus on achieving a strong culture of awareness, respect, and basic knowledge of the opportunities, vulnerabilities and challenges associated with operating in the spectrum. The reason has been summed up often by Dr William Conley, former Executive Secretary of the Electronic Warfare Executive Committee for the US DoD, 2016–2019. 'In five years, I want to be out of a job. Everyone [in the DoD] needs to be treating the EMS like they treat Air. It will be lived and breathed by everyone who has a part in this fight. Then, we won't need the services of an EW EXCOM.'

Mrs Melinda Tourangeau is the Executive Director and Co-Founder of RVJ Institute, a Not-for-Profit Center of Excellence stood up to ensure the US Department of Defense achieves Freedom of Action in the EMS. She graduated from the Georgia Institute of Technology with a BS in Electrical Engineering and completed her MS in Electrical Engineering at Air Force Institute of Technology, with an emphasis on electro-optics and semiconductor physics.

Endnotes

1. International Institute for Strategic Studies (IISS), ‘Military use of the electromagnetic spectrum: the renewed focus on electronic warfare’, The Military Balance 2020 (published online Feb. 2020), https://www.iiss.org/publications/the-military-balance/military-balance-2020-book/military-use-of-the-electromagnetic-spectrum, accessed 16 Mar. 2021.
2. NATO AAP-06, ‘NATO Glossary of Terms and Definitions’, Edition 2020, p. 47.
3. Smith, D. and Tourangeau, S., ‘Denial of Spectrum Denial – NATO’s EW Worry’, Joint Air & Space Power Conference 2020 Read Ahead: p. 119–127.
4. Conley, Todd D., ‘Electromagnetic Interference . . . an Achilles’ Heel’, CHIPS The Department of the Navy’s Information Technology Magazine, (published online Oct.-Dec. 2001) https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=3650#:~:text=EMI%20is%20a%20combination%20of,portions%20of%20the%20electromagnetic%20spectrum, accessed 26 Mar. 2021.
5. Kaul, I., Grunberg, I. and Stern, M., Global Public Goods: International Cooperation in the 21st Century (Oxford University Press: 1999), https://oxford.universitypressscholarship.com/view/10.1093/0195130529.001.0001/acprof-9780195130522, accessed 26 Mar. 2021.
6. Canovas, J., ‘Multi-Domain Operations and Challenges to Air Power’, Joint Air & Space Power Conference 2019 Read Ahead: p. 47–54.
7. Leal-Arcas, Rafael, ‘Sustainability, common concern and public goods’, George Washington International Law Review, no. 49 (2017): p. 87–101.
8. Centre for Collective Action Research (published online Dec. 2018), https://www.youtube.com/watch?v=UawtT2ABfGk, accessed 26 Mar. 2021.
9. University of Gothenburg, Centre for Collective Action Research, https://www.gu.se/en/collective-action-research, accessed 26 Mar. 2021.
10. Jagers, S. C., Harring, N., Löfgren, Å. et al., ‘On the preconditions for large-scale collective action’. Ambio 49, 1282–1296 (2020), https://doi.org/10.1007/s13280-019-01284-w, accessed 26 Mar. 2021.
11. Sell, J., Wilson, R. K., ‘Levels of Information and Contributions to Public Goods‘, Social Forces, Volume 70, no. 1 (1991): p. 107–124, https://doi.org/10.1093/sf/70.1.107, accessed 26 Mar. 2021.
12. Adar, E. and Huberman, B., ‘Free Riding on Gnutella’, First Monday (published online 2 Oct. 2000), https://journals.uic.edu/ojs/index.php/fm/article/view/792/701, accessed 26 Mar. 2021.
13. Ibid. 10.

© Peach ShutterStock/Shutterstock.com

Security Convergence for Air and Space Power

XX

Resilience in Three Dimensions

By Col Dr Eric Trias, US Air Force, and
Col Martin Rothrock, US Air Force
Defense Threat Reduction Agency

Introduction

Looking to the future, the commander of Allied Air Command called for increased efforts to achieve MDO – Multi-Domain Air and Space Operations.[1] Although one of the goals of MDO is to increase resiliency, our reliance on technology to achieve multi-domain operations Command and Control (C2) without a corresponding focus on protection will increase the fragility of critical infrastructure vital to Air and Space (A&S) operations, against enemies developing their own multi-domain capabilities with lethal hybrid warfare strategies. Moreover, threats to A&S operations are becoming increasingly complex as state actor adversaries develop their own multi-domain capabilities not only to physically attack defence critical infrastructure through cyber means, but also to exploit vulnerability of information systems to gain physical access. A promising approach for NATO to assure operations resiliency in the face of this multi-domain threat lies in the concept of convergence of three security disciplines – physical, cyber, and Continuity of Operations (COOP). NATO can no longer depend on cybersecurity alone for operational resiliency, nor can the Alliance rely entirely on guards, guns, and gates to protect critical missions, people, and infrastructure. Comprehensive risk-managed operational practices complemented by diverse, converged security protection programs are needed to meet the challenge.

Why Security Convergence?

Commercial businesses have begun to realize the benefits of converging physical and cyber protection disciplines. A commercial industry survey reports that among Chief Security Officers of worldwide commercial firms with converged physical security and cybersecurity operations, 78 % reported significant benefits to the effectiveness of their security posture.[2] Additionally, commercial industries view convergence of cyber and physical security with COOP, a.k.a. business continuity in industry, as synergistic and highly beneficial. The concept creates an effective response to both natural hazards and manmade threats while creating an effective resiliency posture ensuring mission continuation as a response to both cyber and physical incidents delivering a three-dimensional defence-in-depth protection.

Although physical security has long been deemed essential to preventing unauthorized physical access to critical equipment, assets, or facilities, physical security is often overlooked as vital to protecting all potential access vectors to critical information systems, such as servers or workstations located outside key facilities. Just as effective physical security programs prevent theft, these programs must extend throughout the architecture to prevent data exfiltration or modification by unauthorized users. Gaining physical access to any information system renders even the best cybersecurity measures ineffective, e.g., keyloggers can be planted, systems can be booted surreptitiously using a compromised operating system, or side-channel analysis can be conducted to bypass cryptographic protection. Often critical cyber terrain infrastructure's primary means of protection is through isolation from other networks. However, this 'air-gapped' protection scheme does not guarantee immunity from physical attack, as illustrated by the well-known attack on Iran's Natanz Nuclear Facility by an insider delivering the STUXNET malware through a USB device.[3]

Equally neglected is the perspective of employing cybersecurity to protect modern physical security technology systems is necessary. Evolution of physical security systems transitions proprietary electronic security systems to rely on Internet Protocol (IP)-based architecture as part of the Internet of Things (IoT) technology.[4] IP-based intrusion detection systems along with access and circulation control systems have become increasingly effective and affordable options to protect A&S operations instead of robust military or contracted security forces. However, these systems continue to suffer from widespread vulnerability to cyber threats including weak password practices, poorly protected credentials, improper configuration management, and many even had built-in vulnerabilities which have allowed outsiders to take full control of cameras systems to conduct espionage or utilize them to gain surreptitious access to other networked systems.[5]

Most importantly, security convergence establishes collaboration among the protection disciplines to more effectively defeat the same threats.[6] Consequently, cybersecurity systems and physical security systems (riding on the same network) should employ similar risk management processes and practices. These disciplines both rely on threat assessment, access control, continuous monitoring and rapid response to incidents. As a result, converging security incident response and C2, while using parallel risk management practices, of physical and cybersecurity systems, can more effectively address, prevent, and mitigate potential incidents through predictive analysis.[7]

How to Achieve Convergence Using Risk Management?

In 2020, according to an IBM research, the average cost of a data breach globally and in the US were $3.86 M and $8.64 M, respectively.[8] Even with strong motivations to mitigate risks to address these costs, the global security industry has been slow to eliminate barriers between security disciplines and adopt the concept of convergence. These barriers are likely to be even more difficult for NATO to overcome given the need to achieve consensus among 30 nations. Progress will take time and deliberate effort. However, pragmatic objectives presented here lay out a roadmap for convergence achievable in the next five years. Along the way, utilizing the existing NATO Force Protection (FP) model provides an excellent framework for guiding convergence of cybersecurity, physical security, and COOP programs through a comprehensive risk management process.[9]

The first objective is to improve overall COOP readiness. COOP bridges the gaps between physical security, emergency response, and cybersecurity and provides the greatest improvement of mission resilience for a comparatively modest investment in training and resources. The first step in the NATO FP model, ***mission analysis***, provides the basis for developing more effective COOP to support NATO A&S missions. This process results in identification of the most important assets to accomplish the mission and develops understanding of associated Mission Essential Functions (MEFs) or critical capabilities these assets perform. The resilience against multi-domain attacks can be achieved through establishing redundancy of these capabilities, dispersing physical assets, building alternative procedures, and/or separating mission systems (or critical portions of these systems) from vulnerable networks.

Multiple natural disasters have demonstrated the value of an effective COOP program. However, as the frequency of cyber-attacks increase, organizations must include response to cyber-attacks into their COOP programs. As an example, in 2017, Denmark's Maersk, the world's largest shipping company, became a victim to the NotPetya ransomware devastating its information systems worldwide. Maersk was only able to reconstitute its network, without paying the ransom, due to a fortuitous power outage at an office in Accra, Ghana. Due to the prolonged power outage, the servers were offline when the infected software update propagated throughout Maersk's 108 office in 34 countries. Maersk was able to rebuild its data and administrative systems by physically transporting the Ghana hard drives to the company's headquarters.[10] Although, this specific incident response enabled successful reconstitution of operations, it illustrates the need for an effective COOP process not based on good luck.

The next objective to achieve convergence is to broaden the NATO FP risk management process to embrace a multi-domain approach. Threat assessment, vulnerability assessment, and the risk mitigation responses emerging from this process must be developed through a converged perspective. Broadening the threat assessment aperture is particularly important for NATO because the Alliance faces a hybrid threat increasing in speed, scale, and intensity that combines kinetic attacks from irregular forces with cyber-attacks. However, it won't be easy! NATO faces significant challenges in sharing threat information among Alliance stakeholders and in achieving agreement on threat prioritization, not only due to the 30 nations represented, but just as significantly, to the limited interaction that traditionally exists in military organizations between communications/cyberspace and physical security communities. Additionally, cyber threat information is often classified at a level where it cannot be shared easily among national intelligence services. Nevertheless, NATO must address these challenges to support converged protection of operations. Additionally, use of multi-domain red teams to demonstrate vulnerabilities and development of a Design Basis Threat (DBT) outlining expected adversary cyber, intelligence gathering, and kinetic capabilities can be helpful to achieve consensus on how to robust a security system needs to be and what it is intended to protect against. The NATO FP vulnerability assessment, if conducted with a broader view of multi-domain threats, will inform commanders to consider how both physical and cyber threats can be paired to exploit critical assets to achieve the greatest consequences against their missions. It will show commanders where best to apply multi-domain security resources to achieve a converged defence against hybrid threats.

The NATO threats and hazards identification process identifies the most severe risks to the mission along with countermeasures to consider for reducing risk to an acceptable level. A good example of how this can work for NATO in security convergence is to consider a data centre. In addition to cybersecurity configuration controls and monitoring systems, a data centre supporting an A&S C2 role needs strong physical protections with access control systems, CCTVs, guards, advanced fire protection systems, and redundant utilities for heating and cooling. The ultimate insurance policy for the data centre is a robust, executable COOP plan to answer key questions: Can the alternate site take over all, or part, of the centre's capabilities? Can the MEF's be reconstituted quickly in an alternate location before significant impact occurs? Has the COOP plan been rehearsed? Do adequate resources exist to execute it? When conducting multi-domain A&S operations in a contested environment, these issues are likely to be more important than simply tracking weapon system availability.

Conclusion: The Strategic Challenge

Strengthening COOP and building a multi-domain risk assessment process will get NATO on the road towards dealing with current and future hybrid threats. However, a strategic approach is needed to position NATO to stay ahead of emerging threats. One strategic challenge on the road to convergence is to expand the multi-domain risk assessment model 'outside the wire,' to include assessment of the physical protection, cyber protection, and business continuity programs of commercial infrastructure vital to A&S missions. Another strategic objective, involving changing organizational cultures, is to build a converged mindset among NATO protection professionals in security, cybersecurity, and emergency response disciplines. This can be best accomplished by creating integrated protection units, where personnel are required to train and exercise together to apply their respective disciplines to assure a common mission. Lastly, leadership commitment and championing will be required, along with the support and buy-in of dedicated security professionals.

Convergence shows promise and has been achieved by many large commercial enterprises.[11] It will take deliberate strategy and policies to ensure progress and true convergence occur in NATO. Government organizations and commercial industry must share best practices among stakeholders to expedite adoption and normalization of this security paradigm. The benefits of achieving a three-dimensional security converged environment for mission assurance in a contested multi-domain environment are substantial now, and it will be even more critical in the future to ensure the success of NATO A&S multi-domain operations.

Colonel Eric D. Trias (US Air Force), PhD, is Chief of the Cyber Division, at the Defense Threat Reduction Agency, Nuclear Enterprise Directorate, Mission Assurance Department. He leads all Cyberspace related mission assurance activities in support of Joint Staff directives and DoD assessments of its most critical assets.

Colonel Martin L. Rothrock (US Air Force) is the Chief of the Joint Mission Assurance Assessments Division for the Defense Threat Reduction Agency at Fort Belvoir, Virginia. Col Rothrock is a career Security Forces officer who has commanded at the Squadron, Group, and Wing level.

Endnotes

1. Harrigian, Jeffrey L., 'Shaping the Future Multi-Domain C2', JAPCC Journal, Ed. 29 (2020), p. 6–8.
2. Beck, D., Gips, M., and Pierce, B. M., The State of Security Convergence in the United States, Europe, and India, Alexandria: ASIS International, 2019.
3. Greenberg, A., Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, New York: Doubleday, 2019.
4. Ibid. 2.
5. Bugeja, J., Jonsson, D., and Jacobsson, A., 'An Investigation of Vulnerabilities in Smart Connected Cameras,' IEEE International Conference on Pervasive Computing and Communications Workshops, Athens: 2018, p. 537–542.
6. Ibid. 2.
7. Ibid. 2.
8. IBM Security, 'Cost of a Data Breach Report 2020,' https://www.ibm.com/security/digital-assets/cost-data-breach-report, accessed 26 Jan. 2021.
9. NATO AJP 3.14., 'Allied Joint Doctrine for Force Protection', Apr. 2015, p. 3–6.
10. Ibid. 3., p. 103.
11. Ibid. 2.

© solarseven/Shutterstock.com

NATO Space – Panel Introduction

XXI

NATO's Fifth Operational Domain

By Lt Col Henry Heren, US Space Force
Joint Air Power Competence Centre

Introduction

Many of the most important activities supporting the planning and execution of military operations occur in what has been recently recognized as NATO's highly dynamic and rapidly evolving fifth operational domain, Space. Space-based capabilities are a critical element of all modern militaries. The escalation in Space-related activities has resulted in Space becoming increasingly congested and competitive, with Space-based capabilities being potentially more vulnerable and the domain becoming a priority confrontational area for strategic competitors. To counter threats to Space-based capabilities, it is essential to develop a higher level of Space Domain Awareness and increase the resilience of national Space-based capabilities providing data, products, and services to the Alliance in support of operations. This will require the ability to rapidly replace damaged or inoperable satellites, as well as quickly integrate new capabilities. Plug-and-play ability and modularity are examples of harmonizing these efforts, and of a high level of standardization, fundamental to both reducing the time and cost of production and to altering the decision-making in NATO operations. These new approaches are crucial to the Alliance's ability to maintain access to Space-based data, products, and services, and serve as a strong deterrent to both peer- and near-peer potential adversaries.

Milestones and Progress

While NATO has recently made strides regarding Space by creating an Overarching Space Policy, recognizing Space as an Operational Domain in 2019, establishing a Space Centre in October 2020, and authorizing the creation of a Space-focused Centre of Excellence in January 2021, significant strides have also been made within Alliance Nations.

'The United States had a US Space Command from 1985 until 2002 when … functions were absorbed by US Strategic Command.'[1] On 18 December 2019, the US re-established its Space Command 'to focus on the protection of US Space assets and to strengthen the military's posture in Space as adversaries develop more advanced anti-satellite weapons.'[2] This was followed with 'legislation creating the first new armed service since 1947 – the US Space Force'[3] on 20 December 2019. The focus of the law was to create a 'service that will be totally focused on organizing, training and equipping Space Force.'[4] With the creation of the world's first independent Space Service, the US acknowledged its 'military Space forces must be skilled managers of risk, always seeking mission accomplishment at the speed of relevance while recognizing that perfection is often the enemy of good-enough.'[5]

In early 2020, the UK established 'the Space Directorate, one half of the team specializing in policy and strategy, with the other half being capability focused – based within the MOD in Whitehall.'[6] This was followed by the establishment of 'Space Command, under its own two-star commander, with a focus on doing the day-to-day business of Space. The training of people and generation of expertise, the capability management – delivering programmes and bringing new Space capability to the frontline – and the actual operations of Space, such as managing capabilities we have in-orbit, or running the UK Space Operations Centre.'[7] The current plan is 'direction from the National Space Council will flow through the Space Directorate in MOD Head Office to Space Command and other relevant elements of Defence. It is envisaged that Space Command will interact with the UK Space Agency, as required, to deliver joint national Space capability'.[8]

On 11 September 2020, the French Air Force was officially redesignated 'the French Air and Space Force, completing a process initiated by President Emmanuel Macron in July 2019 when he announced the creation of a Space command'.[9] This follows the 2010 creation of a French Joint Space Command, 'a rather modestly staffed structure but highly positioned in the institution and soon to become a key step in helping Space find its way in the new military thinking'.[10] The French Space Command is in the process of transitioning 'from a mere 30 officer-'Joint Space Command' to a more than 200-uniformed military-organization, before gaining more personnel over time, possibly up to several hundreds'.[11] This recognition of 'the increased French military dependency on Space and the perception of a more hostile environment must be seen as one of the key reasons behind this reorganization'.[12]

From Italy, in the Autumn of 2019, 'the undersecretary of Defense, Angelo Tofalo, and the Chief of Staff of the Italian Air Force, Gen. Alberto Rosso, said that everything is ready to establish the 'General Space Office of Italian Armed Forces.' The first step towards the formation of a Space Command.' Indeed, those first steps have been achieved with the creation of the Italian General Office for Space within the Italian Air Force and consisting of two offices: one focused on innovation and a second on policy and operations. 'As part of the Air Force General Staff, the General Office for Space is configured as the organizational element that manages activities and needs in the Space sector of interest to the Air Force, coordinating both with the internal bodies of the Armed Force.'[13]

NATO Integration of Space-derived Data, Products, and Services (DPS)

As mentioned earlier, last autumn NATO approved the creation of a NATO Space Centre, 'which will serve as a hub for Space-related information, expertise, and activities and directly liaise with the several nations providing Space DPS. Once operational and fully staffed, it will provide greater ability for NATO to coordinate requests for Space DPS.'[14] How the Space Centre, and by extension NATO, will collect, merge, and share relevant Space DPS, particularly regarding Space Domain Awareness, across the Alliance remains to be developed.

Access to and use of Space is currently a very uneven playing field. Some nations are quite advanced in their ability to reach and utilize Space-based capabilities, while others access services through commercial providers only. Similarly, while NATO utilizes Space-based capabilities the associated DPS which they provide are shared by nations who retain authority over the capabilities themselves. NATO must consider how to integrate DPS from the providing nations with the whole Alliance, while the nations who own Space capabilities will execute authorities related to operating those capabilities. This means that NATO must focus on the integration of DPS while the nations focus on maturing organizations, policies, doctrine, exercises, and Space professional personnel.

As Alliance Nations develop and implement policies and strategies for Space operations, NATO must ensure it has access to the DPS those operations generate. At the same time, NATO must seek to develop policies and strategies which maximize the benefit of the nations' expanding capabilities, without seeking to mimic policies and strategies for capabilities which currently, and for the foreseeable future, reside within the nations. NATO seeking an appropriate approach to Space development, compatible to the development within the Alliance, will enable NATO to benefit from Space Power at the speed of relevance.

Additional Articles

This section presents nine related articles which will introduce various ideas and issues related to the Operational Domain of Space, and the different challenges NATO faces therein. The ideas expressed in this article are meant to prepare those attending the 2021 Joint Air & Space Power Conference for the panel discussion on Space:

- The first article, ***NATO Space: International Cooperation is Key to Spacepower***, by General John Raymond (US Space Force), provides a senior leader's perspective regarding the unique challenges facing the burgeoning Space Domain and the crucial role cooperation will play.

- In ***The Role of Space Domain Awareness: Space Asset Resilience thru Protection***, Captain Alessio Di Mare (IT Air Force) discusses the importance of Space Domain Awareness for NATO to continue to have access to Space-derived data, products, and services.

- The next paper, ***Modular Satellite Manufacturing to Enhance Space Assets Resiliency*** is written collectively by Mr Tal Azoulay, Ms Giulia Federico, and Mr Ran Qedar. This paper focuses on approaching the manufacturing of satellites in a modular 'plug and fly' manner to enable greater resiliency across satellite constellations.

- Next, we turn to ***Leveraging Responsive Space & Rapid Reconstitution*** by Mr Bret Perry and Mr John Fuller. This paper explores the benefits of responsive launch capability, especially regarding small satellite constellations.

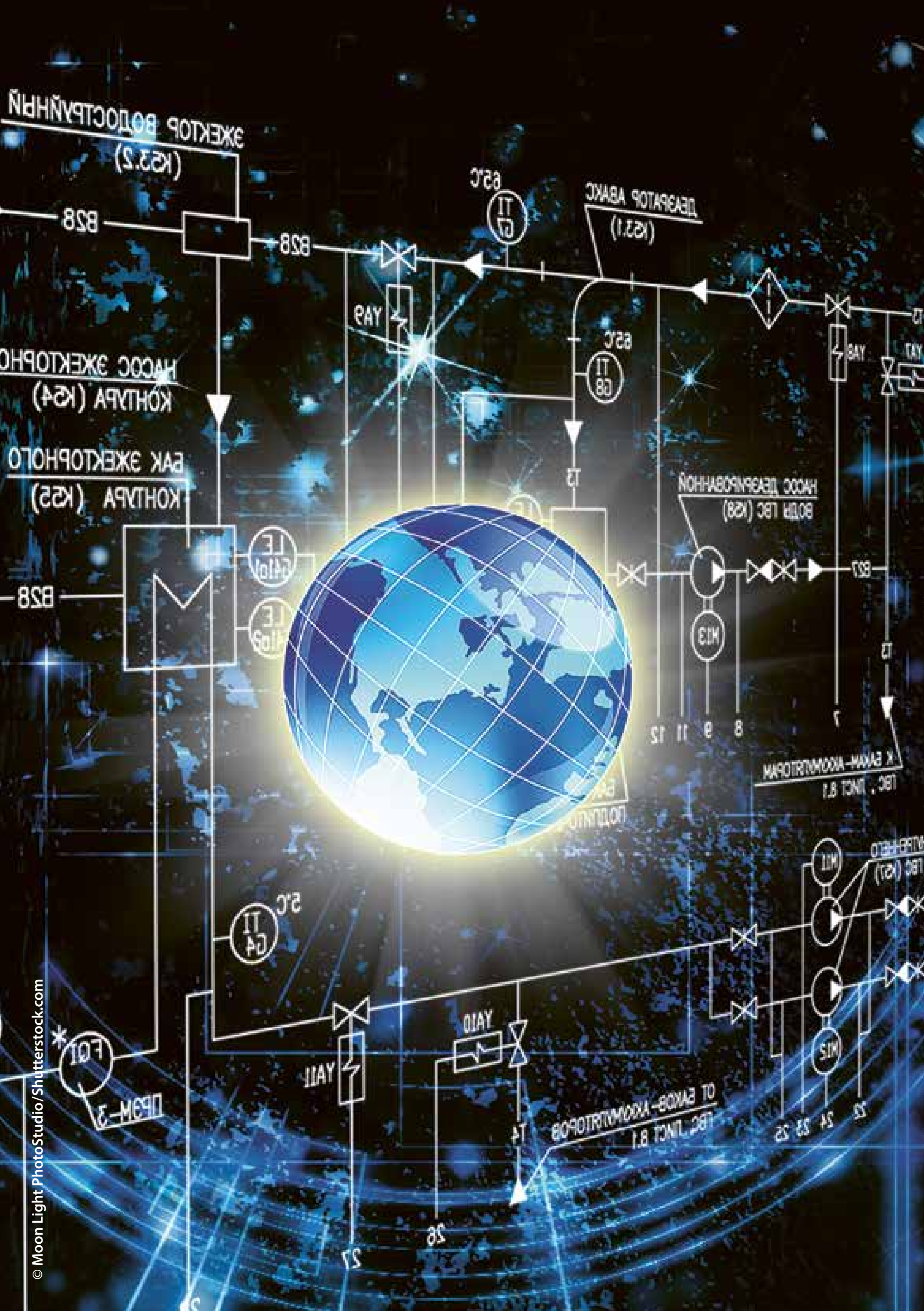
- In ***Chinese 'High-Risk' Corporate Space Actors*** Dr Jana Robinson discusses Space-related economic issues. Specifically, she describes the extend to which Chinese corporations have permeated around the globe as well as implications and recommendations for the Alliance.

- The section is finished by the JAPCC's own Lieutenant Colonel Tim Vasen (GE Air Force) who provides ***From Satellite Generations to a Continuous Evolution***. This work examines a shift in approach to intelligence satellite constellation design, from a generational approach to a continuous improvement of capability with each satellite launched.

Lieutenant Colonel Henry Heren (US Space Force) is a NATO Space & Cyberspace Strategist assigned to the JAPCC. He is a Master Space Operator and a Fully Qualified Joint Staff Officer with operational and planning experience in the Pacific, Europe, Africa, and the Middle East. After more than 28 years of service in the US Air Force, he transitioned to the US Space Force in 2020. He is a graduate of the US Air Force Weapons School, with experience in assignments focusing on Space, Cyberspace, and Electronic Warfare Operations.

Endnotes

1. Erwin, Sandra, Trump Formally Reestablishes US Space command at White House Ceremony, SpaceNews.com. 29 Aug. 2019. Available at: https://spacenews.com/usspacecom-officially-re-established-with-a-focus-on-defending-satellites-and-deterring-conflict/ (accessed on 25 Feb. 2021).
2. Ibid.
3. Garamone, Jim, Trump Signs Law Establishing US Space Force, DOD News. 20 Dec. 2019. Available at: https://www.defense.gov/Explore/News/Article/Article/2046035/trump-signs-law-establishing-us-space-force/ (accessed on 25 Feb. 2021).
4. Ibid.
5. US Space Force, Space Capstone Publication, Spacepower. Jun. 2020, p. 58.
6. Lye, Harry, Q&A: Air Vice-Marshal Harv Smyth talks UK Space Command, AirForce-Technology.com. 23 Feb. 2021. Available at: https://www.airforce-technology.com/features/qa-air-vice-marshal-harv-smyth-talks-uk-space-command/ (accessed on 25 Feb. 2021).
7. Ibid.
8. Royal Air Force, Air Commodore Paul Godfrey announced as Commander United Kingdom Space Command, RAF News. 1 Feb. 2021. Available at: https://www.raf.mod.uk/news/articles/air-commodore-paul-godfrey-announced-as-commander-united-kingdom-space-command/#:~:text=UK%20Space%20Command%20will%20protect,for%20the%20benefit%20of%20all.%E2%80%9D&text=Strategic%20Command%20leads%20on%20developing,air%2C%20cyber%20and%20space%20domains (accessed on 25 Feb. 2021).
9. Mackenzie, Christina, French Air Force Changes Name as it Looks to the Stars, DefenseNews.com. 15 Sep. 2020. Available at: https://www.defensenews.com/global/europe/2020/09/15/french-air-force-changes-name-as-it-looks-to-the-stars/(accessed on 25 Feb. 2021).
10. Pasco, Xavier, Op'Ed: A New French Space Command, ORF Online. 5 Oct. 2019. Available at: https://www.orfonline.org/research/space-alert-volume-vii-issue-4-56195/ (accessed on 25 Feb. 2021).
11. Ibid.
12. Ibid.
13. Italian Air Force, Available at: http://www.aeronautica.difesa.it/organizzazione/loStatoMaggiore/organigramma/Pagine/UGS.aspx (accessed on 15 Mar. 2021).
14. Heren, Henry, NATO Space, Journal of the JAPCC, Edition 31, Winter/Spring 2021. Available at: https://www.japcc.org/nato-space/ (accessed on 15 Mar. 2021).



© Moon Light PhotoStudio/Shutterstock.com

NATO Space

XXII

International Cooperation is Key to Spacepower

By Gen John W. Raymond

Chief of Space Operations, US Space Force

International cooperation in Space has never been more important than it is today. Chinese and Russian military Space activities present serious and growing threats to NATO's security interests due to their development, testing, and destabilizing deployment of counterspace capabilities, along with their associated military doctrine for employment in conflict extending into Space. Although the broader strategic threats posed by China and Russia are different, each has weaponized Space as a means to challenge our freedom of operation in Space and reduce US and NATO military effectiveness. NATO's Space strategy and doctrine should be poised to counter, respond to, and deter the full range of competition and military conflict, including hybrid threats and military activities that fall short of war.

In recognition of this security environment, the United States has reemphasized the importance of international engagement, and the US Space Force is seeking to create greater opportunities for cooperation across

NATO member states and spacefaring partners. The United States is committed to working alongside Allies to deter and defend against aggression from hostile adversaries.[1] In March 2021, the White House released the Interim National Security Guidance, and the continued importance of Space and international cooperation is explicitly highlighted:

> *We will explore and use Outer Space to the benefit of humanity, and ensure the safety, stability, and security of outer Space activities. We will shape emerging technology standards to boost our security, economic competitiveness, and values. And, across these initiatives, we will partner with democratic friends and allies to amplify our collective competitive advantages.*[2]

NATO member states understand that Space is an integral component of their respective national soft and hard power security strategies. By recognizing Space as an operational domain and establishing a new NATO Space Centre at Ramstein, Germany, NATO leaders have acknowledged the increasing counterspace threats posed by potential adversaries.[3] To achieve the security objectives of the Alliance – while ensuring freedom of action in Space – member states and key partners need to lead in the promotion and demonstration of norms of responsible behaviour in Space; promote technological innovation and acquisition agility; mature a transparent attribution process; and develop Space professionals.

Lead in the Promotion and Demonstration of Norms of Responsible Behaviour

The need to define non-binding norms of responsible behaviour for Space operations has considerable international support. Within the United States, policy and strategy documents have highlighted this need as well, to include the most recent National Space Policy that notes the need to promote 'norms of behaviour for responsible national security activities that protect United States, allied, and partner interests in Space'.[4] Also, the US Defense Space Strategy underscores the need to 'join with allies, partners, and other US Government departments and agencies to promote favourable standards and norms of behaviour in Space.'[5] In the second year of the new US Space Force, we are focused on enhancing integration with existing alliances and partnerships, including working toward mutually beneficial tenets for responsible behaviour in Space.

NATO provides a forum to discuss the development of international norms of responsible behaviour for the utilization of Space that consider the changing Space landscape and security implications. This is especially true given the expected growth in Space traffic management, on-orbit servicing assembly and manufacturing, and rendezvous and proximity operations. Collaboratively, the Allies should take actions that enhance Space domain stability and reduce the potential for miscalculations. NATO can promote norms of responsible behaviour in Space favourable to Alliance and key partners' interests. This collaboration could contribute to enhancing the safety and stability of the Space environment to facilitate peaceful exploration, science, and commercial activities.

Promote Technological Innovation and Acquisition Agility

China and Russia continue to develop Space capabilities that reduce the technological advantage long enjoyed by NATO Allies. Failure to innovate, adapt, and become more agile may make the Alliance's Space capabilities less relevant in the near future. In the worst case, disadvantage in Space can create vulnerabilities for Allied forces in multiple domains.

Space Force establishment allowed creation of new organizations and processes to unify complementing Space functions and authorities, already resulting in enhanced security options. To promote greater efficiencies, NATO members could likewise coordinate activities such as cooperative Science & Technology and Research & Development efforts. Working in a coordinated manner, NATO can help ensure our Space capabilities and associate architectures are fully functional throughout the spectrum of peace, deterrence, and conflict.

Prudent risk-taking is inseparable from the concepts of innovation and agility. Military Space forces must be skilled at managing risk, always seeking mission accomplishment at the speed of relevance while recognizing that perfection is often the enemy of good-enough. Protracted acquisition processes can lengthen decision cycles and dilute the transformative potential of proposed innovations. Leaders must continually seek the proper balance between desired capabilities and fielding schedules, between rigour and efficiency, and between deliberation and action.[6] A significant element of Space Force's organizational transformation is creating both the organizational structures and a Service culture that help leaders at all levels balance these complex concerns while addressing an overall imperative for timely action.

Furthermore, to ensure that NATO has the requisite capabilities to be relevant in the future, it is critical to incorporate the innovation experience of the commercial Space sector. The commercial sector – whether satellite operators, launch service providers, or the manufacturing supply base – should play a significant role in NATO's operations and strategy. Commercial Space activities have expanded significantly in both volume and diversity, resulting in new forms of commercial capabilities and services that leverage commoditized, off-the-shelf technologies, and lower barriers for market entry. Together with civil Space agencies with whom we share a common industrial base, the Alliance can leverage innovation and cost-effective investments driven by the private sector, presenting opportunities to develop novel capabilities with a more streamlined and responsive acquisition process. By incorporating the innovation experience of the commercial sector, NATO can implement more effective operations and deterrence strategies, especially as potential adversaries seek to outpace our technological advantage and Space-based capabilities.

Mature a Transparent Attribution Process

A credible, trusted, and transparent Space attribution process – the ability to trace the origin of an action against Space architectures – underpins a successful NATO Space deterrence strategy. Inability to determine the origin or source of a hostile or malicious action undermines the expectation of a credible response.[7] Space Domain Awareness (SDA) is a critical part of attributing threatening or malicious action against Space architectures. SDA encompasses the effective identification, characterization, and understanding of any factor associated with the Space domain that could affect Space operations.[8] The United States has already crafted more than 100 agreements to share situational awareness to support safe satellite operations.

SDA alone, however, may not be enough to enable Space attribution. We must go deeper in our understanding of the domain. We must develop the means to determine the source and pathway of an attack against Space architectures after such an attack has occurred.[9] We need scientific methods to gather data and information from satellites, ground systems, and associated networks regarding actions that are non-kinetic or kinetic, and reversible or non-reversible. For hostile actions in Space, the attribution process may lead to a military response. Yet for less serious acts in Space, attribution may lead to prosecution through civilian courts or diplomatic admonishment.

For the Space attribution process to be viable when needed, NATO Nations must prepare now to develop the requisite SDA and scientific capabilities, rehearse related intelligence collection and information sharing, and integrate trusted commercial partners. By rehearsing the attribution process – such as during combined Space exercises and wargames – it may be determined that additional SDA capabilities are needed. Working together and sharing intelligence and information will lead to increased transparency and build trust and confidence in the Alliance's Space attribution process. This trust and confidence established in peacetime can result in additional countries joining the Alliance's effort during times of crisis.

Develop Space Professionals

The impressive technology that enables spaceflight can sometimes obscure the most important component of Spacepower: our people. Indeed, across NATO's Space community, our greatest assets are the men and women – the Space professionals – who develop, employ, and advance Spacepower. Sound doctrine and superior capabilities are of little use without personnel who have the expertise and empowerment required to wield them. It is of utmost importance that NATO prioritize the development of its Space professionals, ensuring that the Allies' militaries have the leadership, professional expertise, and foresight necessary to protect and defend the Alliance's interests in any future environment, including the Space domain.

Developing Space professionals requires a deliberate process that cultivates a common knowledge base, incorporates professional experience across disparate mission areas, and allows a range of opportunities for leadership advancement.[10] The US Space Force is promoting a number of targeted development efforts to ensure **Guardians**, as well as Allies and partners, develop and maintain a global perspective to provide innovative solutions that are effective and relevant to both national and Alliance security interests. Efforts to develop our professionals, like efforts to develop technology, benefit from cooperation. NATO Space professionals need to be knowledgeable and agile in leveraging the capabilities of the other military services, Allies, and the commercial sector.

Looking Up and Forward

When it comes to protecting common interests in Space, the NATO Alliance is greater than the sum of its individual member countries. The United States recognizes this and is moving to reenergize its arrangement of alliances and partnerships built on trust, democratic values, and shared national interests to address emerging Space-related matters. The US Space Force will do its part in strengthening and standing with our Allies, working with like-minded partners, and pooling our collective strength to advance shared interests and deter common threats. The US Space Force is committed to ensuring Space remains accessible, secure, and stable – for the benefit of not only Americans, but the entire world.

Space has a critical role in international security because all the world's major powers are also Space powers that seek to broaden their use of Space. Given the lessons of history, the strategic advantage derived from Space-based capabilities will not remain unchallenged. The Alliance is well positioned to ensure the needed collective responses to our biggest challenges. NATO can and should play an important role in ensuring peace and stability within the Space domain.

General John W. 'Jay' Raymond is the Chief of Space Operations, United States Space Force. As Chief, he serves as the senior uniformed Space Force officer responsible for the organization, training and equipping of all organic and assigned Space forces serving in the United States and overseas.

Endnotes

1. The White House, 'Interim National Security Guidance', Mar. 2021, p. 19.
2. Ibid., p. 17–18.
3. NATO, 'NATO's approach to space', 23 Oct. 2020, https://www.nato.int/cps/en/natohq/topics_175419.htm.
4. The White House, 'National Space Policy', 9 Dec. 2020, p. 29.
5. US Department of Defense, 'The Defense Space Strategy: Summary', Jun. 2020, p. 8.
6. Headquarters US Space Force, 'Space Capstone Publication, Spacepower', Jun. 2020, p. 58.
7. Gleason M. and Hays P., 'Getting the Most Deterrent Value from U.S. Space Forces', Center for Space Policy and Strategy (2020), p. 3.
8. Ibid. 6., p. 34.
9. Klein J. J., 'Understanding Space Strategy: The Art of War in Space', Abingdon: Routledge, 2019, p. 82.
10. Ibid. 6., p. 47.

© OHB

The Role of Space Domain Awareness

XXIII

Space Asset Resilience thru Protection

By Capt Alessio Di Mare, IT Air Force
Italian Air Staff

Space … a Congested, Contested, and Competitive Domain

In 2018, NATO leaders recognized that Space is a highly dynamic and rapidly evolving environment.[1] As it has happened in other areas characterized by a rapid scientific development, Space technology has developed more quickly than the regulation of the use of Space. In fact, over the last sixty years approximately 9,600 satellites have been placed into Earth orbit[2] without any regulatory framework, and that number is expected to exponentially increase considering the tremendous advances in launch capabilities and spacecraft design. Moreover, the growing number of institutional and commercial actors capable of accessing Space and interested in using it makes Space the focus of increasing competition aimed at obtaining supremacy in the exploitation of this domain. NATO is heavily reliant on Space as it has a major impact on military operations and security activities.

All this led the Alliance to recognize Space as the fifth operational domain (after Air, Land, Sea, and Cyberspace). Since many of the most important activities supporting military operations planning and execution occur in this 'new' domain, it is fundamental to be aware of what happens in Space. Therefore, Space Domain Awareness becomes an essential enabling capacity.

Threats to Space Services and Operations

On 11 January 2007, China 'broke the balance' in Space warfare by firing an SC-19 ASAT missile at its own weather satellite Fengyun-1C. The Space Surveillance Network (SSN) has detected approximately 15,000 pieces of debris coming from that one event, but hundreds of thousands of debris particles (too small to be tracked, but still dangerous for human Space activities and Space operations) were released into Low Earth Orbit (LEO).

In 2009, the collision between the American Iridium 33 (active) and the Russian Kosmos 2251 (deactivated) communications satellites 789 kilometres over Siberia was the first publicly confirmed accident between two intact artificial satellites in Earth orbit.

Since 1957, more than 5,250 launches have resulted in some 42,000 tracked objects in orbit, of which about 23,000 remain in Space and are regularly tracked by the US SSN and maintained in their catalogue, which covers objects larger than about 5–10 cm in LEO and 30 cm to 1 m at Geostationary (GEO) altitudes. Only a small fraction – about 1200 – are intact, operational satellites today.[3] Moving at orbital velocities of thousands of miles per hour, any of these objects could represent a risk for manned and unmanned spacecraft.

The population of charged particles 'trapped' in the layers of the Earth's atmosphere (especially in the ionosphere) such as those coming from the upper atmosphere of the Sun can have impacts on electromagnetic signals and equipment (e. g., radar or radio transmissions problems, degradation in accuracy for positioning, navigation, and timing systems, local breakdowns or in the worst cases, complete loss of service). Solar activities can also disturb satellite orbits, forcing satellite operators to execute manoeuvres in order to recover the right trajectory.

Those just described are only some examples of threats, unintentional and intentional, natural or artificial, that could affect Space systems and operations.[4] It is self-evident how important it is to understand and accurately predict what happens in Space, with particular reference to military operations, where global security and people's lives are at stake.

Space Domain Awareness Capabilities

Given that there is no universally recognized definition, Space Domain Awareness (SDA) can be defined as the capability to detect, track, identify and characterize Space objects and the Space environment, aimed at supporting Space activities in terms of safety, security, and sustainability. We do need to identify risks and threats affecting Space systems in order to take appropriate countermeasures, thereby increasing Space systems resilience.

In practical terms, SDA can be considered the result of the integration of the following capabilities:

a. Space Surveillance and Tracking (SST): detects Space objects, catalogues them, determines and predicts their orbits. This capability itself is divided into three different services:
   - Conjunction Analysis: to deliver collision alerts (consisting of an estimated Probability of a Collision – PoC) between two objects. The

  service is also called Collision Avoidance when a manoeuvre to reduce that PoC is suggested.
  - Fragmentation: to survey and characterize new debris coming from a collision between Space objects or an explosion (e.g. of a rocket body), aimed at rapidly updating the Space object catalogue.
  - Re-entry: to calculate and predict the probable area of impact of Space objects re-entering the atmosphere posing a risk to people and/or infrastructures on the Earth's surface.

b. Space Weather (SWx): studies solar activities and Space environmental effects that can influence performance and reliability of space-borne and ground-based technological systems.

c. Space Intelligence: collects data and information, conducts analysis and exploitation to identify unknown satellites, understand if they are operational and discover their capabilities (i. e., payload discrimination) and purposes (collaborative, hostile, and so on).

Therefore, it could be said that SDA is the same as SSA (Space Situational Awareness, keeping track of objects in orbit and predicting where they will be at any given time[5]) but it would not be correct. Both capabilities arise from the same scientific principles and can use same tools and same sensor networks; but their final goals are different. Specifically, Space Intelligence plays a fundamental role for SDA, whose ultimate goal is to coordinate, command and control Space effects in support of military commanders across the globe, ensuring the availability of a Space service at the right place and right time. Finally, SDA and SSA could be considered as two sides of the same coin; the former is mainly focused on military and operational aspects, the latter on civil/dual uses.

SDA Within NATO Nations

The leading Space actor in the Alliance is the US. They operate the largest fleet of satellites and SSN in the world, managing and maintaining a comprehensive catalogue of Space objects also for the benefit of other countries (Alliance members included). Although a lot of countries can boast some SST/SSA capacity, aside from the US, it is very difficult for a single nation to achieve a complete, effective, and autonomous capacity without cooperation. Some examples are the European Union programme for SST called EUSST (born in 2014) and the European Space Agency (ESA) SSA programme (started in 2009).

A similar reasoning can be made on the topic of SWx; in fact, the American National Oceanic and Atmospheric Administration (NOAA) is the reference agency while, in Europe, the ESA is the point of connection for the capacities of each participating member. NOAA and other cooperative agencies are mainly focused on scientific objectives. Within the Alliance, providing timely and accurate SWx information has been recognized as an important capability to acquire, and it is under discussion to establish a NATO Space Weather Centre (instead of the actual SWx capability as a branch of meteorology and oceanography).

Space Intel also deserves a separate discussion as it is still an undeveloped capability for everyone or, at least, it is probably too small for the task in front of it (as far as it is publicly known[6]). Traditionally, both the military and intelligence communities have seen Space only as a 'tool' for obtaining information. By viewing Space as a domain (potentially a warfighting domain), the need for intelligence about it has increased and includes knowledge on what objects are in Space, where they are, what capabilities they have and what threat they pose to friendly Space systems (ground and user segments included). The US Space Force is planning its first steps toward a new intelligence centre to make the great unknown a little less mysterious. The National Space Intelligence Centre (NSIC) will be an independent organization staffed by highly trained Space subject matter experts capable of providing quality intelligence support to Space warfighters, senior leadership, and policymakers through independent and collaborative work with the current National Air and Space Intelligence Centre (NASIC).[7]

The Present and Future Role of NATO

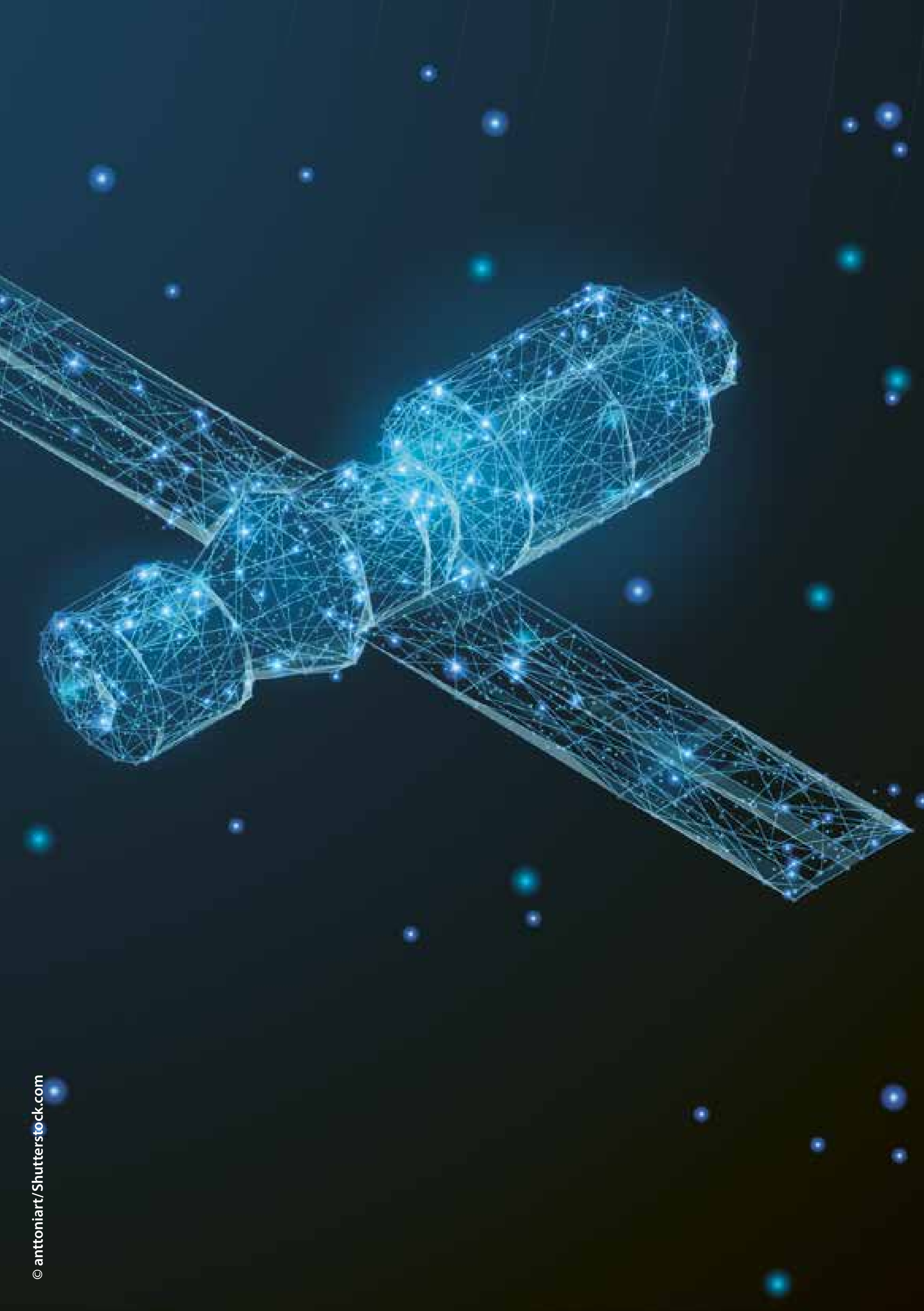
NATO neither has its own Space assets nor operates any. It relies on Space capabilities that Alliance nations provide on a voluntary basis. NATO operations strongly depend on Space services, so SDA also becomes a key resource for NATO and it needs more than just a 'donation' from Member States.

First of all, NATO could be the leading entity to promote the importance of SDA, encouraging the development and improvement of the current architectures and advocating for ideas ranging from the SSA concept of 'simple routine catalogue maintenance' to a tactical, predictive, and intelligence-driven capability integrated with Ballistic Missile Defence and Command and Control infrastructure. Moreover, without jeopardizing the independence of a single nation to use its assets as it prefers, NATO could play the role of coordinator for the various national capabilities, integrating them to have a clearer picture of Space and to be able to detect any change or potential threat on the Alliance, similarly to what happens in civil contexts (e.g., EUSST). Our nations' use of and dependence on Space requires the development of policies and doctrine, tools and resources to maintain the Alliance's superiority in Space. As mentioned before, no country can face this situation alone. The birth of the new NATO Space Centre at Allied Air Command in Ramstein, Germany,[8] could represent the first NATO step in that direction.

Captain Alessio Di Mare (IT Air Force) holds a master's degree in Aerospace Engineering from the University 'Federico II' of Naples and a master's degree in Advanced Communication and Navigation Satellite Systems from the University 'Tor Vergata' of Rome. Since September 2020, he has been working at the General Office for Space of the Italian Air Staff; currently he is head of 'Space Security and Support to Operations' section.

Endnotes

1. Brussels Summit Declaration (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 Jul. 2018).
2. The latest figures related to space debris, provided by ESA's Space Debris Office at ESOC, Darmstadt, Germany. Available at: https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers, accessed 1 Dec. 2020.
3. The European Space Agency, 'About Space Debris', https://www.esa.int/Safety_Security/Space_Debris/About_space_debris, accessed 23 Dec. 2020.
4. For further information: Space Threat Assessment 2019 – A Report of the Center for Strategic & International Studies (CSIS) Aerospace Security Project, Apr. 2019.
5. SSA definition made by Space Foundation. Available at: https://www.spacefoundation.org/space_brief/space-situational-awareness/, accessed 23 Feb. 2021.
6. 'What we really need most is elements of a warfighting domain and military service that have been lacking over the years. We need our own core intelligence capability,' said the new Space Force Vice Commander Lt. Gen David Thompson after his appointment, https://www.c4isrnet.com/battlefield-tech/space/2020/03/11/the-space-force-will-need-space-intelligence/, accessed 3 Mar. 2021.
7. Cohen, Rachel S., 'National Space Intelligence Centre Takes Shape', Air Force Magazine (published online 16 Nov. 2020), https://www.airforcemag.com/national-space-intelligence-center-takes-shape/, accessed 5 Jan. 2021.
8. NATO, NATO Agrees New Space Centre at Allied Air Command, 23 Oct. 2020, https://ac.nato.int/archive/2020/NATO_Space_Centre_at_AIRCOM, accessed 23 Mar. 2021.



© anttoniart/Shutterstock.com

Modular Satellite Manufacturing to Enhance Space Assets Resiliency

XXIV

By Mr Tal Azoulay,
Ms Giulia Federico, and
Mr Ran Qedar
Space Products and Innovation GmbH

Introduction

Space-based assets are a highly strategic element for advanced militaries, to provide critical intelligence as well as command and control. Though this has been accepted for quite some time, recent years have seen a number of countries take further organizational, policy, and operational steps to update their Space outlook. In 2019, Space was declared an operational domain and an official Space policy was agreed on (though it remains classified), advancing NATO Space strategy to meet the present and future challenges. Today NATO's Space capabilities are based on the national assets of various Alliance members. NATO is one of the enduring military Alliances with continued long-term relevance. Operating in Space has become increasingly collaborative in nature, due to the high complexity and elevated costs. Consequently, the NATO framework would make it easier to leverage its Members' relative strengths and capabilities across the Alliance, by executing Space missions in partnership.

Satellites are essential military assets; however, they are extremely fragile and vulnerable. They operate in harsh conditions, with extreme temperatures and almost no protection from physical or cyber-attacks. Their development and deployment timelines are long and expensive, which means that enemies have the time to study their systems and their replacement is not immediate. In a nutshell, they represent a low-risk/high-reward military target. Disaggregation or rapid replacement of Space assets have been some of the most effective strategies to mitigate Space vulnerabilities.

The current problem is that Spacecraft production is often a very long and expensive process. It takes years to assemble a satellite that will last at maximum up to 15 years. The requirements for satellite systems have remained unchanged in the past ten years.[1] Satellite manufacturers use customized systems limiting spacecraft design options, in a process that is long, expensive, and complex. Satellite system resiliency is compromised by the current state of the manufacturing cycle and for scale production up to 80 % of the costs go to contractors to supply customized systems when the actual cost is only 20 %.[2] This cost for customization is due to the lack of interoperability between the suppliers since there is no single standard for hardware and software communication. Integrating components from a myriad of manufacturers presents a challenge that until now could result in significant increases of production time and costs.

The ability to build a satellite with plug-and-play subsystems, as one would build Lego, would open new avenues of interoperability and enable mission program flexibility. This capability has been recently developed in the form of a compact universal adapter that would allow this plug-and-playability. The bottom line is that satellites production times and costs can be reduced significantly while increasing project flexibility and overall Space capability resilience.

Evolving Spacecraft Domain

Recent years have seen a significant shift in geopolitical dynamics, leading to uncertainty and the increasing need for Western alliances to adapt quickly to evolving threats in the international arena.[3] For the Space domain this can be seen with growing concerns with regards to the development and deployment of anti-satellites capabilities. Large and small countries alike are developing national defence postures to include Space and increasing the amount of military cooperation in this field. These trends generate a demand for rapid responses to unclear scenarios and Space-based intelligence platforms can provide additional clarity for decision-makers.

NATO members are facing a rapidly changing environment, with an increasing need for operational readiness and systems resiliency. A recent JAPCC publication presented the argument that NATO should 'exert its political influence to ensure that Alliance nations apply resilience concepts for the development of their Space systems' … and '… should strongly foster the selection of resilient, redundant, and synergetic national Space systems – commercial solutions included – to support NATO operations.'[4]

One way to achieve a resilient Space infrastructure is enabling satellite scale production to allow the replenishment of depleted or damaged resources in a shorter amount of time by increasing the manufacturers' ability to provide the same product in a fraction of the time without compromising on the quality. 'Maintaining a robust infrastructure to service or quickly replace disabled satellites will be critical. These are all ingredients of an effective deterrence by denial.'[5]

NASA has recently issued a call for Batch-Producible Small Spacecraft that will serve as its next-generation fleet of multi-mission spacecraft.

This trend comes from the adoption of the commercial market of serial production of small satellites by new Space companies such as SpaceX, OneWeb, BlackSky, and more, that are utilizing more efficiently these compact satellites compared to the traditional industry.

An accelerated pace of technological and capability advancements increases the likelihood that a new technology will be available for a spacecraft during its development time. Whether or not that new capability will be implemented in the spacecraft will depend on the platform's flexibility and ability to rapidly incorporate unplanned hardware without negatively impacting the project timeline. As Space companies are spread more around the globe, a prime contractor working to produce a Space system is more likely to be required to integrate a variety of subsystems and components from a multitude of sources that are not coordinated between themselves in terms of standards and protocols. True plug and play opens more doors by making it easier to cooperate with various manufacturers.

NATO's primary modus operandi is based on interoperability of its members, 'Future NATO and national systems must be interoperable. Furthermore, NATO should ensure commercially procured services are interoperable with Alliance systems'.[6] That said, developing a single standard for Space components is a complex and long-term idea with no resolution on the immediate horizon. However, there are increasing options in terms of component providers and the evolving threat arena demands immediate solutions. Considering the above, the ability to conveniently integrate bespoke components will be a valuable advancement.

A Plug and Fly Solution

The concept of conveniently compatible subsystem integration has been examined in various iterations over the years. Militaries as well as the Space industry recognized the inherent value that this would provide in production of spacecraft. The last major project that was implemented to reduce the time to assemble a satellite using plug and play technology was the PnPSat-1 project initiated in 2004 by the United States Air Force Research Laboratory. While the project eventually managed to assemble a satellite in 4 hours, this was after significant efforts were made towards standardization of components, implementation of new design, and qualifying of subsystems under the new standards.[7] The US DoD has estimated that it would require $1 Billion to implement a new unified standard on all existing hardware and software that is in development for next-generation Space programs.[8]

Connectivity between digital systems on-board a satellite can require up to 20 different interfaces on the hardware and a larger amount on the software protocol for communication. This is due to the heritage of components coming from different domains or organization types (government, agency, commercial, university, other industries) and the unique closed solution that each satellite manufacturer solves with its supply chain (around 25 worldwide).[9]

A cost-efficient solution is required to bridge the standardization gap in satellite electronics in order to increase component compatibility and achieve faster and more flexible production of satellites. One approach proposed to achieve modularity and plug and play is to utilize a universal and intelligent data node as an intermediate layer between satellite On-Board Computer (OBC) and its subsystem/payload. The data node behaves like a smart data router to connect various units of the satellite to the OBC. Holding a database of subsystem drivers, the node will

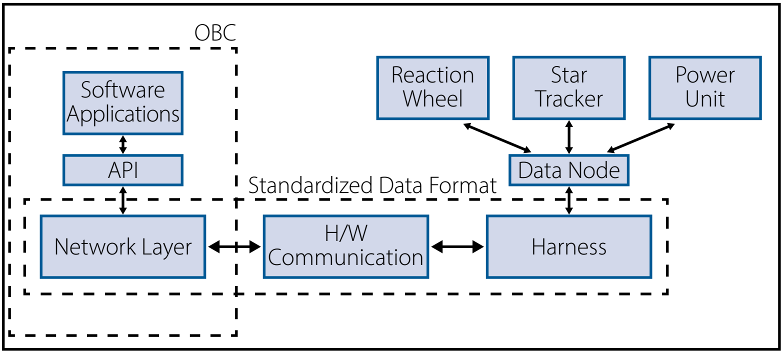


Figure 1: *Satellite architecture with intelligent data node.*[11]

enable smart functionalities such as device recognition, self-configuration, and driver installation.[10]

The advantage of this solution is that manufacturers will be able to use current systems off-the-shelf and integrate them through the data node without the need for hardware customization or system integration. This plug-and-play data node enables satellite modularity and flexible architecture, reducing costs and time of satellite manufacturing enabling satellite scale production, effectively achieving a complete plug and fly solution. Systems suppliers will also benefit from it, thanks to its hardware and software compatibility, suppliers will be able to provide their hardware to a wider number of manufacturers, overcoming design limitations. The data node can be placed anywhere on the bus and systems can be plugged and unplugged at any time. During the satellite assembly phase, faulty systems can be replaced immediately without consequences.

Furthermore, this solution also enables faster technology cycle and the testing of new payloads, by lowering the cost of the satellites and allowing faster and automatic integration of new systems into existing ones.

Conclusions

Modern warfare is more dependent than ever on Space infrastructure to provide critical intelligence, communication, and command and control. Modular satellites integrated through plug-and-playable data nodes provide a cost-efficient solution that delivers rapid replacement capabilities, shorter innovation cycle and support for new mission concepts. The current trend of Space agencies, military commands, and new Space companies to support serial production creates opportunities to cross-utilize subsystems technology, sharing resources between domains that until now worked independently. NATO deserves simple but advanced technologies that will help it confront emerging challenges in the 21st century as a 21st century Alliance.

Mr Tal Azoulay attained his BA in Political Science from Stony Brook University in New York, and his MA in Security Studies from Tel Aviv University in Israel. As a Space policy researcher specializing in the fields of international cooperation and conflict resolution, he has lectured and published on these topics. Since 2020 he is the Business Developer of Space Products and Innovation GmbH.

Ms Giulia Federico graduated in 2012 from the University of Rome La Sapienza with a master's degree in International Relations and Diplomatic Studies. She worked at the Earth Observation Coordination Office and at the Communications Department of the European Space Agency. Since 2015 she is the Chief Operations Officer of Space Products and Innovation GmbH.

Mr Ran Qedar received a BSc from the Technion in aerospace engineering in 2009 and his MSc in space system engineering from TU Delft in 2015. He has more than ten years of experience in the field of space systems engineering, including testing, integration, software development and operations. Since 2015 he is the Chief Executive Officer of Space Products and Innovation GmbH.

Endnotes

1. Werner, Debra, 'How long should a satellite last', SpaceNews (published online 24 May 2018), https://spacenews.com/how-long-should-a-satellite-last, accessed 29 Jan. 2021.
2. Magistrati, G., 'Data Systems and On-Board Computers, Roadmap – Issue 4 rev. 2', Industrial Policy Committee, Technology Harmonisation Advisory Group Roadmap Meeting, 2016, European Space Agency.
3. NATO, NATO 2030: United for a New Era, 25 Nov. 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf, accessed 29 Jan. 2021.
4. Console, Lt. Col. Andrea, 'Space Resilience – Why and How?', Journal of the JAPCC, Issue 27 (13 Mar. 2020): p. 10–16, https://www.japcc.org/space-resilience-why-and-how/, accessed 29 Jan. 2021.
5. Paulauskas, Dr Kestutis, 'Space: NATO's latest frontier', 13 Mar. 2020, https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html, 29 Jan. 2021.
6. Single, Maj. Thomas, 'Consideration for a NATO Space Policy'. In ESPI Perspectives, #12 (2008), https://www.files.ethz.ch/isn/124746/espi_perspectives_12.pdf, accessed 29 Jan. 2021.
7. Wikipedia, 'PnPSat-1', 13 Jan. 2021, https://en.wikipedia.org/wiki/PnPSat-1, accessed: 28 Jan. 2021.
8. AFRL Project Lead of PnPSat-1, 'Personal conversation'. 8 Sep. 2020.
9. Space Products and Innovation GmbH (2015). Feasibility Study with Satellite Manufacturers Primes.
10. Conference paper, Plug and Fly, Saish Sridharan, Ran Qedar, 70th International Astronautical Congress (IAC), Washington DC, USA, 21–25 Oct. 2019.
11. Qedar, Ran; Sridharan, Saish, and Federico, Giulia, Space Products and Innovation GmbH, 2016, Intelligent data node for satellites, European Patent Office, EP3293922A1.

© IgorZh/Shutterstock.com

Leveraging Responsive Space and Rapid Reconstitution

XXV

Enabling Resilient Space-Based Data, Products, and Services for NATO

By Mr Bret Perry and
Mr John Fuller
Virgin Orbit

Introduction

As NATO's reliance on Space-based Data, Products, and Services (DPS) grows, NATO member countries face a more contested Space domain with new kinetic and non-kinetic threats. While Space becomes increasingly contested, Space technology is simultaneously advancing with the proliferation of small satellites that are easily reconstitutable. The ability to affordably and responsively replace small satellite constellations will serve as a strong deterrent to adversaries, thanks to the ease and speed by which disabled capabilities can be restored. As then-Chief Marshall of the United Kingdom (UK) Royal Air Force (RAF) Sir Stephen Hiller explained in 2018, 'The prospect of cost-effective constellations of small satellites being built, launched, and replaced quickly is hugely exciting, providing us with the resilience that we seek.'[1]

This capability, known as Responsive Space, yields tactical and strategic benefits that can enhance NATO's access to Space-based DPS capabilities. Tactically, Responsive Space enables the rapid establishment of technologies in orbit, rapid reconstitution of disabled assets, rapid deployment of new constellations, and obscuring launch activities from adversaries. Strategically, Responsive Space alters decision-making in Space warfighting, and can enable resilience for NATO Space-based DPS assets. A key requirement for Responsive Space is having a launch capability that can be rapidly mobilized to offer operators with greater control over the launch origin, with sufficient performance to provide a high degree of launch windows and orbits. Such flexibility is only truly offered by an air-launch system in contrast to existing, fixed-infrastructure launch systems.

This paper will introduce how NATO member countries can employ disaggregated small satellite architectures underpinned by Responsive Space to preserve Space-based DPS capabilities. The benefits of achieving Responsive Space and how they can be enabled via horizontal air-launch will be explored. Finally, this paper will examine how NATO member countries can achieve a Responsive Space capability using a global network of allied spaceports.

Employing Reconstitutable Small Satellite Constellations for NATO Space-Based DPS

NATO's declaration of Space as an operational domain occurred during a unique time in which Space technology is simultaneously advancing with the advent of capable small satellites that are relatively inexpensive compared to traditional monolithic platforms. The United States (US), UK, France, Norway, the Netherlands, Luxembourg, and other NATO member countries are all exploring small satellite applications for various Space-based DPS missions. Blackjack, BRIK-II, ARTEMIS, and other initiatives exemplify how NATO member countries with established and emerging Space capabilities can enhance access to Space-based DPS via small satellites. As explained by US Air Force General John Hyten, disaggregation of 'juicy targets' into distributed networks of satellites can help achieve Space resiliency.[2]

NATO member countries can further maximize the mission impact of small satellites by deploying them into tailored non-traditional orbits now easily accessible via newly-developed dedicated launch systems. Deploying small satellites into novel orbits across multiple orbital planes enables more frequent revisit and enhanced coverage over an area of interest. For example, a constellation of eight small satellites deployed into eight orbital planes at a critically inclined 'Magic Orbit' can provide coverage over an area of interest for 87% of the day, unlocking a meaningful disaggregated and resilient communications or Positioning, Navigation, and Timing (PNT) capability.[3]

An increase in constellation deployments by NATO member countries to provide more Space-based DPS will create more demand for responsive launch capabilities to enable satellite replenishment. Rapid reconstitution reduces the need to keep spare satellites on orbit, minimizes gaps in coverage when satellite capabilities degrade, and allows refresh of technology in a much quicker timeframe. As detailed in the US Space Force's **Spacepower** doctrine, 'during conflict, Space launch must be dynamic and responsive, providing the ability to augment or reconstitute capability gaps from multiple locations.'[4]

The Benefits of Responsive Space for Enabling Resiliency

Responsive Space yields a broad set of tactical and strategic benefits that can enhance the activities of NATO member countries in Space and enable resilience. One unique tactical benefit of Responsive Space is the ability to rapidly deploy a new system. A mobile air-launch system can be deployed from a myriad of existing airports regardless of current system deployment locations and mobilized to rapidly launch a constellation of new satellites. Access to these multiple horizontal launch sites can provide NATO member countries with the ability to inject the satellite directly into its orbit to minimize the time in between launch and a satellite constellation's collection over a target. When coupled with a network of spaceports within different NATO countries, multiple viable pathways to orbit exist and can be quickly activated.

Another tactical benefit of a disaggregated horizontal air-launch system is the ability to provide multiple mission origination locations that can hinder adversarial response to the deployment of new Space capabilities. For example, via loitering or switching among different potential release zones, an air-launch platform provides thousands of daily launch solutions when compared to vulnerable fixed-site launch infrastructure. Thousands of different origination points with little downrange land overflight can be pre-planned and executed at will as part of any mission scenario, offering a flexible launch capability that can deter or delay an adversarial response.

These tactical benefits roll up into a broader strategic impact that expands the Space decision-making landscape. Traditionally, Space warfighting operations have been dictated by the long lead times and the predictability of Space activities – operations in Space require known sequential dependencies that are defined by the laws of physics and orbital mechanics that cannot be disobeyed. Horizontal launch transforms this dynamic as it allows for planners to add far more situational variables, such as access to orbit from numerous launch sites and a reduced timeline to execute. This ability provides NATO member countries an increased set of Space effects that can be implemented to control the Space domain.

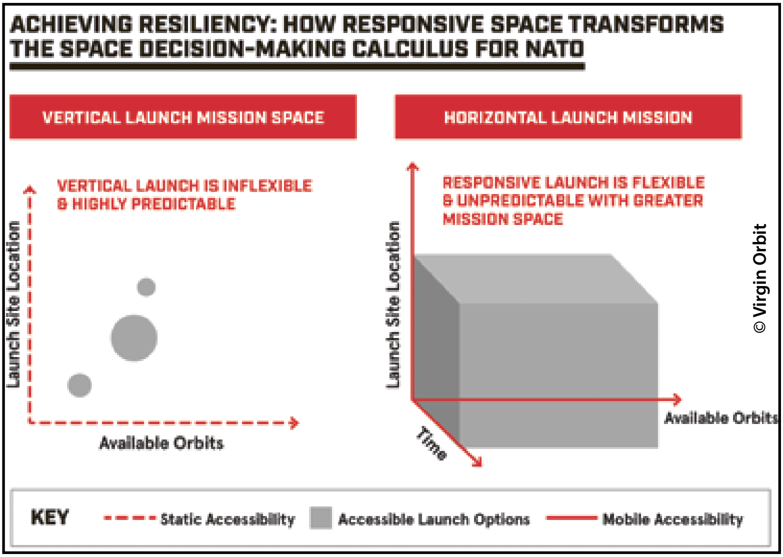

ACHIEVING RESILIENCY: HOW RESPONSIVE SPACE TRANSFORMS THE SPACE DECISION-MAKING CALCULUS FOR NATO
VERTICAL LAUNCH MISSION SPACE
HORIZONTAL LAUNCH MISSION
VERTICAL LAUNCH IS INFLEXIBLE & HIGHLY PREDICTABLE
Launch Site Location
Available Orbits
RESPONSIVE LAUNCH IS FLEXIBLE & UNPREDICTABLE WITH GREATER MISSION SPACE
Launch Site Location
Available Orbits
Time
© Virgin Orbit
KEY
Static Accessibility
Accessible Launch Options
Mobile Accessibility

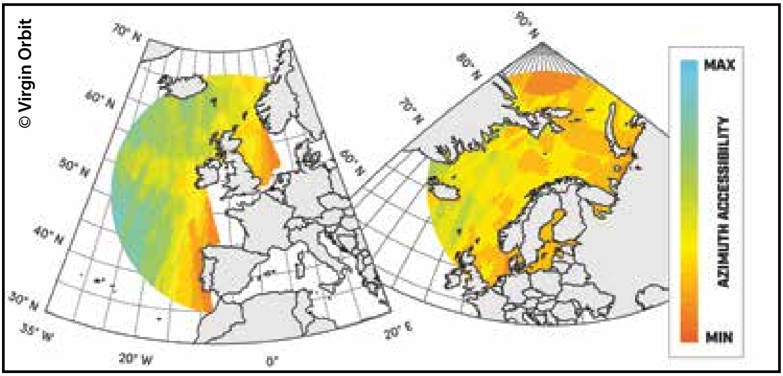
Figure 1: *Horizontal Launch Mission Space vs Vertical Launch Mission Space.*

With these benefits, Responsive Space unlocks strategic deterrence and resiliency in space for NATO allies. Deterrence is an effect that both enables and benefits from resiliency in the Space domain. With Responsive Space, adversaries will recognize that pursuing hostile activities in Space will not yield the desired end-state without increasing their exposure to costly retaliation.

Responsive Space Facilitated by NATO European Horizontal Launch Infrastructure

Air-launched systems are now authoritatively proven to be deployed responsively from austere locations around the world with minimal infrastructure.[5] Horizontal launch operations can be implemented rapidly to bring orbital access to nearly any NATO member country at any airport near a coastline with a sufficiently long runway. Typical air-launch operations generally require a concrete apron large enough to accommodate the carrier aircraft that is displaced from heavy traffic or other airport personnel. Most international commercial airports or government airbases can accommodate such a need.

Spaceport feasibility analytical tools show that horizontal launch from NATO member countries would enable turnkey domestic launch activities with a great degree of orbital access to many inclinations.[6] A region extending to the north and west of continental Europe was analyzed while assessing launches to inclinations ranging between 60° and Sun-Synchronous Orbit (SSO); lower inclinations are possible with increased rocket reliability or extended aircraft range. Northern and southern departure azimuths were considered, resulting in tens of thousands of simulated and evaluated air-launch trajectories. These trajectories were then evaluated for acceptably low risk in casualty expectation to populations they overflew using US Federal Aviation Administration (FAA) risk models.

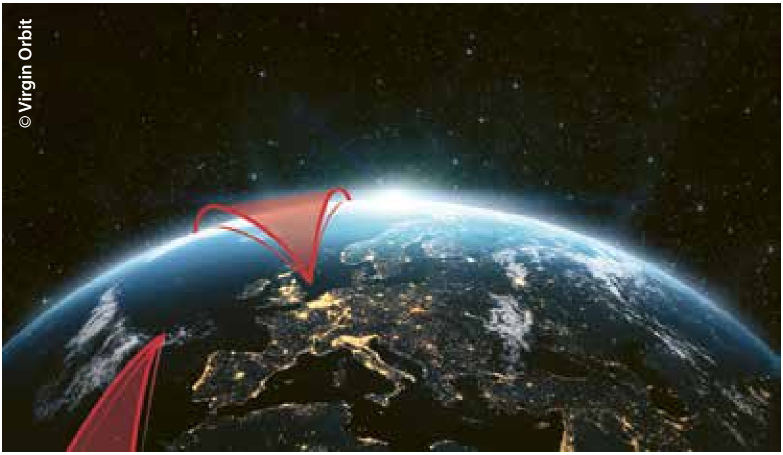


© Virgin Orbit

Figure 2: *NATO European Region Inclination Access via Horizontal Air-launch.*

Figure 2 shows an azimuth access rating map that adheres to a casualty expectation lower than the maximum allowable conditional 'Expected Casualty' of 1 x 10-4 by the FAA for launch licensing in regulating allowable launch activities; the Expected Casualty is a calculation that aggregates risk to the uninvolved public downrange of the rocket launch from impacting vehicle in the event of an anomaly. Regions with most favourable access between 60° and SSO are indicated by the colour bar. Blue regions indicate the ability to launch to all inclinations in the considered range, while orange and red indicate launch is possible to fewer inclinations.

Figure 3 depicts examples of orbital access corridors showing launch envelopes to inclinations between 70° and SSO from the North Sea, and 80° and SSO from the Atlantic Ocean. Lower inclinations can be reached by reaching release sites further from shore. These regions are readily accessible to most NATO member countries, and the access is further enhanced by potential launch from overseas territories and bases.



© Virgin Orbit

Figure 3: *Horizontal Air-Launch Orbital Access Corridors near NATO European Member Nations.*

Table 1 provides a preliminary list of most of the NATO member countries that have existing airports in proximity to these regions. Some NATO member countries have more than one potential airbase or can utilize overseas territories to expand their orbital access. Such examples are the Portuguese Azores, French Guiana, Dutch Curaçao, and various UK overseas stations (Ascension, Diego Garcia). When envisioning a disaggregated network of spaceports capable of rapid or simultaneous air-launch activities, it has been shown that powerful small satellite constellations can be constructed within days or less.[7] Such a framework would involve two or more NATO launch carrier aircraft and their associated mobile support equipment, stationed among any combination of compatible spaceports. The result is a disaggregated and unpredictable launch network that can be activated at a moment's notice.

Conclusion

Given the discussed advancements in small satellite technologies and prospective horizontal launch infrastructure, NATO member countries are in a unique position to capitalize on these developments to build out a resilient Space architecture for existing future Space-based DPS. NATO member countries can pool resources to leverage their respective domestic industrial capabilities, collaboratively building out this global Space ecosystem. NATO member countries could begin doing so by formally assessing which airports (including those in Table 1) could be configured to accommodate a horizontal launch capability and studying the CONOPs for joint responsive launch operations out of these sites. Existing multilateral initiatives such as the Responsive Space Capabilities Memorandum of Understanding, already signed by seven NATO member countries, serve as an example of how this can be done.[8] Ultimately, this growing international interest in Responsive Space creates an opportunity for NATO member countries to develop architectures that leverage shared allied investments in this capability.

Member Country	Candidate Spaceport	Approximate Orbital Access
Albania	Kuçovë Airbase	80° to SSO (Atlantic)
Belgium	Ursel Airbase	70° to SSO (N. Sea, Atlantic)
Bulgaria	Burgas Airport	80° to SSO (Atlantic)
Canada	Mirabel Airport	80° to SSO (Arctic)
Croatia	Dubrovnik Airport	80° to SSO (Atlantic)
Denmark	Karup Airbase	70° to SSO (N. Sea, Atlantic)
Estonia	Ämari Lennubaas Airbase	70° to SSO (N. Sea, Atlantic)
France	Istres-Le Tubé Airbase	70° to SSO (N. Sea, Atlantic)
France	Cayenne-Félix Eboué Airport	0° to SSO (French Guiana)
Germany	Rostock-Laage Airport	70° to SSO (N. Sea, Atlantic)
Iceland	Keflavík International Airport	60° to SSO (Atlantic, Arctic)
Italy	Taranto-Grottaglie Airport	80° to SSO (Atlantic)
Latvia	Riga International Airport	70° to SSO (N. Sea, Atlantic)
Netherlands	Amsterdam Airport Schiphol	70° to SSO (N. Sea, Atlantic)
Netherlands	Curaçao	0° to SSO (Equatorial)
Norway	Andoya Spaceport	70° to SSO (Norwegian Sea)
Poland	Malbork 22nd Airbase	70° to SSO (N. Sea, Atlantic)
Portugal	Santa Maria Airport (Azores)	50° to SSO (Atlantic)
Spain	Gran Canaria Airport	50° to SSO (Atlantic)
Turkey	Balıkesir Airport	80° to SSO (Atlantic)
United Kingdom	Newquay Airport (Spaceport Cornwall)	70° to SSO (N. Sea, Atlantic)
United Kingdom	Overseas Stations (e.g., RAF Ascension Island)	0° to SSO
United Kingdom	Various Airports/Airbases (e.g., Anderson Air Force Base)	0° to SSO
* Nations requiring further analysis: Czech Republic, Hungary, Greece, Lithuania, Luxembourg, Montenegro, North Macedonia, Romania, Slovakia, and Slovenia		

Table 1: *NATO Member Countries who have Potentially Compatible Airports that Enable Orbital Access via Horizontal Air-Launch.*

Mr Bret Perry is a Business Development Principal at Virgin Orbit, where he focuses on helping international governments and commercial operators fulfil their launch requirements. Previously, Bret worked at Avascent, where he provided critical support in strategy development for clients in the aerospace and defence sectors. Bret holds a Bachelor of Science in Foreign Service from Georgetown University.

Mr John Fuller is the Director of Advanced Concepts at Virgin Orbit. John has been with Virgin Orbit since 2016, and is responsible for the conceptual, financial, and competitive evaluation of developmental programs. Prior to joining Virgin, he worked at Orbital ATK. John holds Bachelor of Science and Master of Science degrees in Aerospace Engineering from North Carolina State University.

Endnotes

1. Pultarova, Tereza, 'UK military looking at smallsats to increase space resilience', SpaceNews (published online 23 May 2018), https://spacenews.com/uk-military-looking-at-smallsats-to-increase-space-resilience, accessed on 29 Jan. 2021.
2. Erwin, Sandra, 'STRATCOM chief Hyten: 'I will not support buying big satellites that make juicy targets', SpaceNews (published online 19 Nov. 2017), https://spacenews.com/stratcom-chief-hyten-i-will-not-support-buying-big-satellites-that-make-juicy-targets, access on 29 Jan. 2021.
3. Developed by the Aerospace Corporation, a 'Magic Orbit' is a critically inclined (63.4°) elliptical orbit with a perigee at 525 km and apogee at 7,800 km. These characteristics enable a prolonged dwell time over a targeted area of interest. For further information, please see: 'Magic Orbit' Wertz, James, 'Coverage, Responsiveness, and Accessibility for Various "Responsive Orbits"'. In AIAA Responsive Space Conference (3rd) [conference proceedings]. Los Angeles, C.A., 2005 [cited 17 Jan. 2021). Available at: https://smad.com/wp-content/uploads/2005/04/rs3_wertz_2001.pdf.
4. United States Space Force Headquarters. Space Capstone Publication Spacepower, Arlington: 2020.
5. Vasen, Tim, 'Responsive Launch of ISR Satellites'. In JAPCC Journal (Issue 37) [electronic journal]. Kalkar, Germany, 2018 [cited 20 Jan. 2021), available at: https://www.japcc.org/responsive-launch-of-isr-satellites/
6. Fuller et al., 'Modularized air-launch with Virgin Orbit's LauncherOne system: Responsive smallsat constellation construction measured in hours, not months'. In AIAA/USU Conference on Small Satellites (33rd) [conference proceedings]. Logan, U.T., 2019 [cited 21 Jan. 2021), available at: https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4442&context=smallsat.
7. Ibid.
8. The Responsive Space Capabilities Memorandum of Understanding is a joint research and development multilateral initiative with defence scientists from Australia, Canada, Germany, the UK, Italy, the Netherlands, New Zealand, Norway, and the US. For further information and an example project, please see: Lingard et al., 'Demonstration of a Heterogeneous Satellite Architecture during RIMPAC 2018'. In AIAA/USU Conference on Small Satellites (33rd) [conference proceedings]. Logan, U.T., 2019 [cited 3 Mar. 2021), available at: https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4448&context=smallsat.

© Brian A Jackson/Shutterstock.com

Chinese 'High-Risk' Corporate Space Actors

XXVI

By Dr Jana Robinson

Prague Security Studies Institute

Introduction

A significant, and continuously increasing, number of Chinese enterprises are being sanctioned or officially designated as, in effect, 'bad actors' by the United States and Japan through such venues as the US Department of Defense Section 1237 List of 'Communist Chinese Military Companies' (CCMCs), the US Department of Commerce 'Entity List', the Treasury Department's Office of Foreign Assets Control (OFAC) sanctions list and the Japanese Ministry of Economy, Trade and Industry's 'End User List'.

The first tranche of companies on the Pentagon's list of CCMCs was released on 25 June 2020. The list, originally commissioned by Congress in 1999 pursuant to Section 239 of the National Defense Authorization Act, includes companies with extensive ties to the Chinese Communist Party (CCP) and the People's Liberation Army (PLA). They include companies involved, for example, in the illegal building and militarization of man-made islands in the South China Sea, advanced weapons manufacturing and proliferation concerns, human rights abuses, cyberattacks, mass surveillance, etc.

On 14 January 2021, the Department of Defense added nine new CCMCs (fourth such tranche of companies), now totalling 44 companies.[1] Of those, 18 have been identified as Space-related (i.e., involved in manufacturing, distribution and sale of Space infrastructure, or Space-related equipment, products, and services).

This article provides a list of these Space-related CCMCs, a map of their global corporate footprints and offers risk profiles for four of these State-Owned Enterprises (SOEs) as case studies. It then describes the implications for the Space domain of China's deployment of the SOEs as power projection vehicles to advance Beijing's national strategy (often described as Military-Civil Fusion), including its military Space objectives. Finally, the research findings seek to help illuminate the largely overlooked subject of Economic and Financial (E&F) dimensions of Space security as practiced, and successfully leveraged, by China. Given the limited scope of the article, it could not treat the networks of publicly traded and other subsidiaries of these companies (a number of which are also under US sanctions). For example, the 18 Space-related companies referenced have over 2,000 subsidiaries, many of which warrant close, security-minded scrutiny.[2]

Global Footprints of Chinese Space Companies on the Pentagon CCMC List

The Chinese SOEs are vehicles of a new brand of soft power projection. Their activities often combine both commercial and strategic interests. Unlike their Western counterparts, Chinese companies often operate using non-market terms and conditions (e.g., subsidized financing, etc.) Moreover, many decisions pertaining to overseas investments are subject to direction and approval by the Chinese government.

As mentioned above, out of the 44 companies on the Pentagon's so-called Section 1237 List of CCMCs, at least 18 operate in the Space sector (see Table 1). As of February 2021, the Prague Security Studies Institute (PSSI) has identified 260 transactions in 87 countries by the 18 Space-related companies on the Pentagon's CCMC List. Out of those, 21 were identified as Space-related business transactions in Asia, Australia, Europe, the Middle East and South America.[3]

Space-Related Companies on US Department of Defense 'Communist Chinese Military Companies' (CCMC) List
Aero Engine Corporation of China
Aviation Industry Corporation of China (AVIC)
China Academy of Launch Vehicle Technology (CALT)
China Aerospace Science and Industry Corporation (CASIC)
China Aerospace Science and Technology Corporation (CASC)
China Communications Construction Company (CCCC)
China Electronics Corporation (CEC)
China Electronics Technology Group Corporation (CETC)
China International Engineering Consulting Corp. (CIECC)
China North Industries Group Corporation (Norinco Group)
China Spacesat Co., Ltd.
China Telecommunications Corp.
China United Network Communications Group Co Ltd
CRRC Corp.
Dawning Information Industry Co (Sugon)
Inspur Group
Luokong Technology Corporation (LKCO)
Panda Electronics Group

Table 1: *Space-Related Companies on the US Department of Defense 'Communist Chinese Military Companies' List (As of February 2021) (PSSI).*

Space-related Companies on Pentagon List	MSCI ACWI (All Country World Index)	iShares MSCI ACWI ETF (ACWI)	MSCI ACWI EX-US INDEX	iShares MSCI ACWI EX-US ETF (ACWX)	MSCI EM (Emerging Market) INDEX	iShares MSCI EM ETF (EEM)	FTSE EM INDEX	VAN-GUARD FTSE EM ETF (VWO)	S&P Emerging Market BMI INDEX	SPDR Portfolio Emerging Market ETF (SPEM)	Frankfurt Stock Exchange
Aviation Industry Corporation of China (AVIC)			●	●	●	●	●	●	●	●	●
China Aerospace Science and Industry Corporation (CASIC)											●
Inspur Group					●	●	●	●	●	●	
China United Network Communications Group Co Ltd	●										●
CRRC Corp.	●	●	●	●	●	●	●	●			
China Aerospace Science and Technology Corporation (CASC)											●
Aero Engine Corporation of China					●		●	●			
Panda Electronics Group								●	●	●	●
Dawning Information Industry Co (Sugon)					●	●	●	●			
China Telecommunications Corp.	●	●	●	●	●	●	●	●	●	●	●

Table 2: *Presence of Space-Related CCMCs in indexes and index funds often held by US and European investors as well as having a presence in the Frankfurt Stock Exchange (FSE) (RWR Advisory Group[17] and Börse Frankfurt[18]).*

Sample Risk Profiles

The risk profiles of four of the SOEs appear below (i.e., the Aviation Industry Corporation of China, the China Aerospace Science and Technology Corporation, the China Aerospace and Industry Group Corporation, and the China Electronics Technology Group Corporation). This exercise is designed to demonstrate that such companies are 'high-risk' from a security perspective and their presence often indicates a desire by Beijing to advance its industrial plans and influence, or even outright capture, the Space sectors of their international Space 'partners'.

AVIC, CASIC and CASC are also funded on US and European capital markets. Concerning this latter point, below is a partial list (see Table 2) of the indexes and Exchange-Traded Funds that hold these and other Space-related CCMCs as well as their presence on the Frankfurt Stock Exchange (FSE).

AVIC

The Aviation Industry Corporation of China (AVIC), established in April 1951, develops and produces military equipment for the PLA's Air Force (PLAAD), PLA Naval Air Force (PLANAF), and PLA Rocket Force (PLARF) and is also active internationally through the acquisition of foreign companies, and production/sale of aerospace equipment, etc. AVIC and its subsidiaries have been sanctioned on five separate occasions by the US for activities that played a key role in developing Iran's missile capabilities and other proliferation activities (e.g., Sudan,[4] etc.) AVIC and its subsidiaries[5] have designed and manufactured weapons systems capable of attacking surface combat vessels in the South China Sea.

There have been concerns about supply chain risks related to AVIC's European acquisitions. In July 2013, for example, AVIC acquired Germany's

Thielert Aircraft Engine, scuttling its active involvement in European defense industry.[6] AVIC is publicly traded in the US and European capital markets and 26 of its subsidiaries are listed in Hong Kong, Shenzhen, and Shanghai.

CASIC and CASC

The China Aerospace and Industry Group Corporation (CASIC), together with the China Aerospace Science and Technology Corporation (CASC), are the two key drivers of China's Space industry. They are both wholly owned by the Chinese government and, as such, fall under the supervision of the State-Owned Assets Supervision and Administration Commission (SASAC) of the State Council and the State Administration of Science, Technology and Industry for National Defense (SASTIND).[7] SASAC enables the government and the CCP to intervene in the business, management, and investments of these enterprises.

CASIC and CASC direct the operations of their many respective subsidiaries.[8] For example, CASC's subsidiary, China Great Wall Industry Corporation (CGWIC), is one of its trading arms and stated to be the only commercial entity that is authorized by the Chinese government to provide 'commercial satellite launch services and Space technology to international clients'.[9] It was also identified in PSSI's research as China's most active Space entity globally in both the number and value of transactions (notably in developing countries such as Laos, Venezuela, etc.).[10]

CASIC, founded in 1956, is the primary contractor of the Chinese Space program.[11] It is the domestic leader in missile equipment development, Space launch vehicles and other Space systems (including anti-satellites capabilities such as high-power lasers.)[12] In April 2016, CASIC was identified by the Subcommittee on Terrorism, Nonproliferation, and

Trade in the US House of Representatives as supporting Pakistan's ballistic missile program.

CASC was established in 1999 and, among many other activities, has carried out Chinese efforts to gain a foothold for its companies in Europe through the establishment of special industrial and/or free trade zones. A prominent example is the 'Great Stone Industrial Park' complex outside Minsk, Belarus, where CASC agreed to become the 'anchor company' in March 2018.[13]

CETC

The China Electronics Technology Group Corporation (CETC) is China's leading military electronics manufacturer founded in 2002 by the merger of numerous research institutes managed by the Ministry of Information Industry. It is China's flagship company for design, production, integration, and implementation of command and control systems for the international market and it operates in over 100 countries, including a European headquarters in Graz, Austria. The company collaborates with the Technical University Graz and the University of Technology Sydney, Australia. CETC, together with CASIC and other entities, was behind China Galileo Industries Ltd, formed in 2004 to develop the civilian use of the EU's global navigation satellite system,[14] and subsequently developing a competing system, BeiDou, declared fully operational in the summer of 2020.

The company has been implicated by the US Department of Justice in at least three cases of illegal exports of technology and several of its research institutes and subsidiaries are on the US Department of Commerce's Entity List and the Japanese 'End User List'.[15] CETC's surveillance technology is being used to monitor Muslim Uyghur citizens in Xinjiang, including those in mass detention camps.

Implications for Allies

China's growing Space presence globally is often driven by objectives of the CCP and the PLA. State-owned enterprises, in effect, weaponized by the Chinese government, have, to date, forged Space partnership arrangements with some 60 countries globally. Low-cost launch services and heavily subsidized Space infrastructure development and financing are taking market share from European and US Space companies at quite an alarming rate, not to mention bringing China greater influence in multilateral Space fora.

There has been little, if any, coordinated allied response to this E&F behaviour through NATO or elsewhere. Compounding this problem is the ironic fact that scores of millions of unwitting European and American retail investors are funding these Chinese corporate 'bad actors' through the purchase of their stocks and bonds (for those which are publicly traded).

Conclusion

NATO should be more alert to this ground-based Space race being prosecuted by China through its state-controlled enterprises on a largely uncontested basis. They are successfully creating for Beijing politically exploitable Space dependencies, expanding its influence to shape global Space standards and norms and advancing its vast military Space program.

To date, US-sanctioned Chinese Space-related companies have never faced allied penalties of any kind, even in the category of unfair trade practices. Executive Order 13959,[16] issued by the previous US Administration in November of last year, made these 18 Space companies and others on the Pentagon's CCMC List legally off-limits to all US investors globally, as they are prohibited from holding the securities (i.e., stocks and bonds) of these companies effective 11 November 2021. NATO would benefit from better understanding the serious knock-on effects of this first-time use of capital markets sanctions by the US.

NATO also needs to help maintain a level commercial and financial playing field in the Space domain, where economic and financial leveraging techniques are routinely employed by Beijing, in order to prevent the capture of the fledgling Space sectors of smaller nations.

Dr Jana Robinson is Managing Director at the Prague Security Studies Institute (PSSI). She also serves as Director of PSSI's Space Security Program. Prior to this post, she held the position of a Space Policy Officer at the European External Action Service (EEAS) in Brussels. From 2009 to 2013, she led the Space Security Research Program at the European Space Policy Institute, seconded from the European Space Agency. She holds a PhD from the Charles University's Faculty of Social Sciences, Institute of Political Studies.

Endnotes

[1] 'DOD Releases List of Additional Companies, In Accordance with Section 1237 of FY99 NDAA'. In Defense.gov [online], 2021 [cited 17 Feb. 2021). Available at: https://www.defense.gov/Newsroom/Releases/Release/Article/2472464/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/.

[2] Data based on 'IntelTrak Data'. In RWR Advisory Group [online]. 2021 [cited 3 Mar. 2021). Available at: (subscription only): https://www.rwradvisory.com/inteltrak/.

[3] As referenced above, these data points do not include the over 2,000 subsidiaries of these 18 companies. For any comprehensive analysis, these subsidiaries would have to be thoroughly researched.

[4] 'GLOBAL TRADE, LOCAL IMPACT Arms Transfers to all Sides in the Civil War in Sudan'. In Human Rights Watch [online], 1998 [cited 18 Feb. 2021). Available at: https://www.hrw.org/legacy/reports98/sudan/Sudarm988-05.htm#P577_102736.

[5] AVIC has over 100 subsidiaries.

[6] 'AVIC acquires Thielert Aircraft Engines'. In Pilotweb.aero [online], 2013 [cited 18 Feb. 2021). Available at: https://www.pilotweb.aero/news/avic-acquires-thielert-aircraft-engines-1-2295681.

[7] Mu R., Fan Y., 'An Overview of Chinese Space Policy'. In Schrogl KU., Hays P., Robinson J., Moura D., Giannopapa C., 'Handbook of Space Security' (2015). Springer, New York, NY: p. 413–430.

[8] Capital Trade Incorporated, 'An Assessment of China's Subsidies to Strategic and Heavyweight Industries'. In US-China Economic and Security Review Commission [online], 2009 [cited 18 Feb. 2021). Available from: https://www.uscc.gov/research/assessment-chinas-subsidies-strategic-and-heavyweight-industries.

[9] 'China Great Wall Industry Corporation (CGWIC)'. In Nti.org. (n.d.) [online], 2001 [cited 18 Feb. 2021). Available at: https://www.nti.org/learn/facilities/50/.

[10] Robinson, J., Robinson, R., Davenport, A., Kupkova, T., Martinek, P., Emmerling, E., and Marzorati, A., 'State Actor Strategies in Attracting Space Sector Partnerships: Chinese and Russian Economic and Financial Footprints'. In Prague Security Studies Institute [online], 2019 [cited 17 Feb. 2021). Available at: http://www.pssi.cz/download/docs/8177_686-executive-summary.pdf.

[11] 'About CASC'. In China Aerospace Science and Technology Corporation [online], 2018 [cited 18 Feb. 2021). Available at: http://english.spacechina.com/n16421/n17138/n17229/index.html.

[12] https://www.uscc.gov/sites/default/files/Research/USCC_China-Space-Program-Report_April-2012.pdf.

[13] 'China Aerospace Science and Technology Corporation to open research center in Belarus'. In Belta.by [online], 2018 [cited 18 Feb. 2021). Available at: https://eng.belta.by/society/view/china-aerospace-science-and-technology-corporation-to-open-research-center-in-belarus-113476-2018/.

[14] Mulvenon, J, and Tyroler-Cooper, R. S., 'China's Defense Industry on the Path of Reform' In US-China Economic and Security Review Commission [online]. 2009 [cited 18 Feb. 2021). p. 46. Available at: https://www.uscc.gov/sites/default/files/Research/REPORT_DGI%20Report%20on%20PRC%20Defense%20Industry111009.pdf.

[15] 'China Electronics Technology Group Corporation' In China Defence University Tracker [online]. 2020 [cited 18 Feb. 2021). Available at: https://unitracker.aspi.org.au/universities/china-electronics-technology-group-corporation/.

[16] 'Executive Order 13959: Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies'. In FederalRegister.org [online]. 2020 [cited 1 Mar. 2021). Available at: https://www.federalregister.gov/documents/2020/11/17/2020-25459/addressing-the-threat-from-securities-investments-that-finance-communist-chinese-military-companies.

[17] RWR Advisory Group (2020). 'The US Capital Markets Footprints of the Pentagon's "First Tranche" List of PLA-Affiliated Chinese Enterprises Operating in the United States'. In RWR Advisory Group [online]. 2020 [cited 3 Mar. 2021), p. 1-19. Available at: https://www.rwradvisory.com/wp-content/uploads/2020/07/RWR_Pentagon_List_Report.pdf.

[18] 'Börse Frankfurt–Equities'. In boerse-frankfurt.de [online]. 2021 [cited 3 Mar. 2021). Available at: https://www.boerse-frankfurt.de.

© Sergey Nivens/Shutterstock.com

From Satellite Generations to a Continuous Evolution

XXVII

Discussing a Paradigm Change in the Design and Operation of ISR Satellite Constellations

By Lt Col Tim Vasen, GE Air Force
Joint Air Power Competence Centre

Classical developments of military technology and equipment follow a generational approach. For example, if a nation wants to develop a constellation of Intelligence, Surveillance and Reconnaissance (ISR) satellites which consists of 5 satellites, they usually develop the whole constellation, launch the satellites in a relatively short timeframe and operate it for a calculated lifespan (usually between seven to fifteen years). After a certain timeframe, based on the calculated lifespan and the experience gained during the operational phase, the follow-on system gets projected and the process starts again.

Evolving technology as well as decreasing launch costs should encourage nations to follow a different approach. Referred to in this paper as the 'continuous constellation approach' and using the example of the five satellite constellation as stated above, the constellation will not be built up as a generation package and launched simultaneously, but will incorporate evolving technology into the development of each individual satellite in turn. This allows for periodic replacement of the oldest satellite on orbit with the most current technology available, in a continuous rotation. Due to the significantly reduced launch costs, which have been a limiting factor in the past, the calculated lifespan of each satellite could be reduced, allowing for more frequent launch of smaller satellites with lower technical redundancy rates while still ensuring safe continuous operations. The continuous regeneration with up to date technology provides a large advantage over the long term. This article discusses one specific idea to keep an ISR constellation functioning at 'the speed of relevance'.

Examples in the Development of Recent Military ISR Constellations

Traditional projected development, launch, and use cycles of ISR constellations usually follow approaches similar to these examples:

The German SARLupe military ISR satellite constellation was initiated in 1998. The specifications[1] were formulated in 2000 and industry partners were awarded contracts in December 2001. 2006 saw the first launch, with the full constellation of five satellites completed in 2008.[2] Designed with a ten-year lifespan, the constellation is still operational while the follow-on system, SARah (whose conceptual work led to an industry contract in 2013), is already delayed from 2019 to late 2021.

The conceptual development of the Italian COSMO SkyMed dual-use constellation started in 1998,[3] involving the Italian Ministry of Defense in 2001. The first satellite was launched in 2007 with a designed lifespan of 5.25 years. The constellation of four was finished in 2010 and all satellites are still operational. The development of the follow-on generation started in 2011 with a contract awarded to industry partners in 2015. The first satellite was launched in 2019.

When compared to the German SARLupe, the gap between the designed end of life of the first generation and the launch of the follow-on system of the COSMO SkyMed constellation could have been even more significant. Both constellations can be seen as blueprints for the long timelines between idea, acceptance, design, build, and launch of an ISR satellite constellation in western governmental processes.[4]

Risking a New Paradigm: Small and Inexpensive Satellite Solutions, Based on Commercial Off the Shelf Technology

Maintaining technical developments at the speed of relevance with Space systems is an important, but extremely difficult enterprise. Even when developments of military technology which results in the fielding of systems to the armed forces follow a slower path than the integration of technical developments in the civilian world, Space systems are unique in this aspect, too. While equipment used in the Land, Air, Maritime and Cyberspace domains can be upgraded with software and hardware components, Space-based systems have only a limited option to receive and incorporate software upgrades. Limited in this context means that there is no chance to upgrade or even repair the electronic components once launched. Therefore, redundant elements that allow a longer lifespan in Space have to be integrated. These electronic components, when certified and designed for long term usage in Space, usually offer lower performance than equipment designed to be used on the Earth.

In most western countries, satellite constellations operated in generations as described earlier, are the norm. Due to these long term processes and high launch costs, the aim in the past was to design a constellation with a projected lifespan as long as possible. A longer projected lifespan requires an increased redundancy rate for components, specifically for the use in Space certified electronic components, as well as a larger amount of fuel to sustain the orbit over a longer timeframe. These stringent requirements lead to higher costs due to specifically designed components that possess a higher survivability rate in Space which further leads to higher launch costs due to increased satellite weight. Finally, if you consider a one to three-year production process, the 'age' of the technology at the end of the designed lifetime of a satellite, which has been on-orbit for seven to fifteen years, is then between eight and eighteen years. In the author's opinion, this is not in keeping with the 'speed of relevance' from a technical perspective.

Discussing a New Paradigm

The question then is how government procured ISR satellite constellations can keep pace with evolving technological developments? In endeavouring to answer that question, this paper will discuss an approach referred to as 'the continuous constellation approach.' This means changing the focus from longer lifespans and pre-defined constellations to a more flexible approach. Risking shorter lifespans of individual satellites offers decreased launch weight due to reduced redundancies and thus lower fuel needed for orbit sustainment.

Technological Considerations

The 'lower redundancy' approach involves using commercial off the shelf technology to produce small and modular satellites that will be operated via a standardized process. The payloads can be adjusted prior to the launch to react to security and intelligence needs. To maintain the speed of relevance, each modular satellite will be technically up-to-date, based on available technology, prior to being launched. This is especially applicable for hardware related to data storage, data transmission and on-board computing.

For the overall design of a continuous constellation, the change in the mindset is to focus on capabilities, not on assets. Transitioning from a pre-planned to a modularity plug and play satellite design, offers a maximum of flexibility.[5] This can integrate modular payloads that can be technically upgraded or converted prior to launch, such as switching the payload from an electromagnetic sensor to an electro-optical one or vice versa. There are already examples of this approach in commercial satellites that are built utilizing off-the-shelf technology components, which are offered at very low prices.[6]

Actual technical options allow an electro-optical ground resolution of one meter that can be achieved by unpropelled satellites with a launch mass of less than 50 kg.[7] Satellites in that resolution regime with propulsion systems have a launch mass of roughly 120 kg.[8] Unpropelled ISR satellites equipped with a submeter SAR payload can be built with a launch mass of roughly 100 kg each.[9] A propelled system with a comparable payload has a launch mass of roughly 150 kg each.[10] Unpropelled satellites, equipped with a Signal Intelligence (SIGINT) payload, are available with a launch mass of less than 70 kg.[11] Satellites with these specifications are already successfully used on orbit and are, in the author's opinion based on their performance, usable for military purposes. The designed and achieved lifetimes vary between two and four years for unpropelled and between three and six years for propelled satellites.

Launch Schedule Approaches and Orbit Selection

An initial disadvantage of this approach is the longer timeframe between the initial launch and the full operational capability of a constellation, since the satellites are launched at larger intervals compared to the classical approach where satellites were built in parallel and then launched en masse in a shorter timeframe. However, once the buildup of the initial constellation is complete for this continuously launched approach, likely with one to three launches per year based on the constellation's design and security requirements, the subsequent steady-state replenishment schedule (one to two launches per year for a constellation of four satellites, for example) will offer much greater flexibility. This approach is able to launch the needed payload in the regular launch cadence that is projected and will have the chance to launch responsively additional assets if needed.

Launcher and Launch Opportunities

The current developments on the launcher market offer opportunities to be more flexible. Inside the NATO alliance there are several developments of small launchers on-going that have the chance to be used for national launches of smaller satellites. For example, the use of an Electron launcher, provided by the US-NZL company Rocket Lab© which can carry 300 kg into Low Earth Orbit (LEO) costs between $5 and $7 Million.[12]

A standard Falcon 9 launcher provided by the US company SpaceX© costs $62 Million, but is able to carry up to 22 tons into LEO.[13] This should offer affordable ride-share solutions, which means using available launch mass for secondary payloads that are not used by the primary payload. The disadvantage is that the launch is optimized for the prime customer and the secondary payloads have to arrange themselves around those requirements.

Using these two opportunities gives nations options to launch systems cost-effectively, mainly on a ride-share basis. This is particularly true if there is no threat or security requirement impeding the action, and via small individual launches to react quickly or to close gaps in constellation coverage as needed.

These two launchers are examples for affordable launch services that have challenged the previous providers and nearly squeezed some of them out of the market. Worldwide there are more than ten other launchers capable of launching between 300 kg and 1.5 tons currently under development and will have their maiden launches within the next few years.

Overall Assessment and Chances

Smaller satellites with a shorter designed lifespan reduce the production costs tremendously. This cost reduction compensates for the higher amount of launch costs due to a higher launch rate. Continuously upgrading the systems prior to launch, based on recent technical developments, will increase the individual satellite's performance over time. This also allows the operating nation to have a continuously upgraded constellation which can react to changing payload requirements with modular designs and to enhance regional focus with specific orbits to gain better coverage on an area of interest when necessary while only slightly reducing coverage on other areas of the world.

Postscript

From the author's perspective, the definition of a system like this which could have an operational and usable time that is unlimited when supported by continuously upgraded replenishment on orbit, may become critical in government internal fiscal planning for systems acquisitions. A financial forecast and planning for decades can limit the courageous approach as discussed here. However, even these requirements can be modified over time and could be viewed as slower than the processes described for the lifecycles of the classical constellation as stated above.

Lieutenant Colonel, DipEng, MSc. Tim Vasen (GE Air Force) served in positions responsible for IMINT planning and technical assessments, including positions at the office of military studies as a senior analyst for Space systems and head of Space intelligence at the German Space Situational Awareness Centre (GSSAC). Since October 2017 he serves as Space Intelligence SME at the JAPCC.

Endnotes

1. 'Bundeswehr belauscht die Welt', Spiegel Politik Online, (published online 1 Sep. 2009) https://www.spiegel.de/politik/deutschland/strategische-aufklaerung-bundeswehr-belauscht-die-welt-a-575417.html, accessed 13 Mar. 2021.
2. Gunter Krebs, 'Gunter's Space Page', https://space.skyrocket.de/doc_sdat/sar-lupe.htm accessed 12 Mar. 2021.
3. European Space Agency (ESA), 'ESA Earth Observation Portal', https://directory.eoportal.org/web/eoportal/satellite-missions/c-missions/cosmo-skymed, accessed 10 Mar. 2021.
4. Similar examples can be found in nearly all western nations such as France, Great Britain, Canada, USA and Japan.
5. Also discussed as an option in 'Technology Horizons', US Air Force technology study released in 2010, covering the years from 2010 to 2030.
6. The US company Planet© sustains since 2014 the 'Flock' constellation which consists of mass-produced inexpensive satellites which are continuously upgraded due to technical components that are accessible off the shelf. Several hundred of these 5 kg satellites have been launched since then, ensuring a continuously usable constellation of 100+ assets in Space.
7. Gunter Krebs, 'Gunter's Space Page', https://space.skyrocket.de/doc_sdat/nusat-1.htm, accessed 8 Mar. 2021.
8. Gunter Krebs, 'Gunter's Space Page', https://space.skyrocket.de/doc_sdat/skysat-3.htm, accessed 1 Mar. 2021.
9. Gunter Krebs, 'Gunter's Space Page', https://space.skyrocket.de/doc_sdat/capella-2.htm, accessed 4 Mar. 2021.
10. Gunter Krebs, 'Gunter's Space Page', https://space.skyrocket.de/doc_sdat/harbinger.htm, accessed 9 Mar. 2021.
11. Gunter Krebs, 'Gunter's Space Page', https://space.skyrocket.de/doc_sdat/hawkeye.htm, accessed 12 Mar. 2021.
12. 'Deutsche Raumfahrtfirma chartert Kiwi-Rakete – für geheimnisvollen Kunden', Spiegel Wissenschaft Online, (published online 13 Jan. 2021), https://www.spiegel.de/wissenschaft/weltall/ohb-deutsche-raumfahrtfirma-chartert-kiwi-rakete-fuer-geheimnisvollen-kunden-a-df65540b-7c65-4c87-a5b2-45e47a4d391c, accessed 14 Jan. 2021.
13. SpaceX, 'Capabilities & Services for the Falcon 9 and Falcon Heavy rocket family´, https://www.spacex.com/media/Capabilities&Services.pdf, accessed 25 Feb. 2021.

Joint Air Power Competence Centre
JAPCC

The Executive Director's Closing Remarks

Lt Gen Klaus Habersetzer, GE Air Force
Executive Director, Joint Air Power Competence Centre

It is my hope that the individual papers provided in our Conference Read Ahead have been thought-provoking and illuminating. Our goal is to inspire and elicit discussion during our upcoming conference concerning the role of Joint Air and Space Power in NATO. As the Executive Director of the Joint Air Power Competence Centre (JAPCC), I wanted to take this opportunity to offer my perspective and underscore some elements of the theme of this year's conference focused on Delivering NATO Air & Space Power at the Speed of Relevance.

In the summer of 2020, when we were first developing the theme for the 2021 Conference, we were uncertain as to the lasting impact of the ongoing global pandemic. The challenges associated with COVID-19 have expedited the development and use of new ways to execute missions on behalf of the Alliance in ways previously not considered or even possible.

With a growth in NATO's mission set and the return of what is being referred to as great power competition, the necessity to harmonize NATO policy and strategy is more important than ever. The increased use of information age capabilities allows threats to reach the Alliance from around the world. This new reality in no way reduces traditional threats from peer and near-peer competitors, to the contrary, it exacerbates the potential risks. The Alliance continue to find a balanced approach to meet any challenge, which starts with fostering consensus and providing clear guidance to the member nations.

Once the strategic guidance is provided, NATO military forces must be prepared and equipped to communicate and operate across the operational domains. Adversaries will seek to limit NATO's ability to respond to threats, and so NATO must be ready to execute decision-making process in a dynamic targeting environment. This ability will rely heavily upon new technological capabilities, empowered by artificial intelligence and machine learning, coupled with innovative approaches to command and control across all domains.

And it is not only the technologies which are ever-expanding, but also NATO's reach. In late 2019 NATO recognized Space as its fifth operational domain. As NATO seeks to establish its intent and explore opportunities derived from Space, the Alliance Nations are also increasing their focus outside of Earth's Atmosphere. As the nations organize and re-organize their capabilities and approaches to Space, NATO must also adapt its ability to coordinate with the nations to maximize Space support to NATO operations. This will include not only a growth of appreciation and understanding for Space capabilities within NATO, but also potentially an increase in Space professional personnel and an expansion of mission and roles within NATO organizations.

From the strategic- to the tactical level of operations, across all domains, the Electromagnetic Spectrum (EMS) is crucial to all modern military operations. The ability to utilize the EMS in a contested and congested battlefield requires Electronic Warfare (EW) to both attack adversary capabilities and protect Alliance forces and missions. While all NATO forces utilize the EMS, none are perhaps more reliant on the EMS than those associated with Cyberspace operations. Understanding how NATO can utilize EW to exploit the EMS and ensure operations across domains is a critical capability, one which NATO ignored for too long and is only now beginning to reconsider in earnest.

The themes covered in these papers are certainly not all-inclusive, but they represent the most inclusive and comprehensive JAPCC Conference Read Ahead ever published. The collected papers, all originally written for this collection, are from military and civilian service members, academic and civilian think thanks, and our industry partners from around the globe, which includes authors from action officers to senior leaders. I invite you to visit our conference website to further explore details regarding the panels, the topics, themes, and the registration process for this year's conference: https://www.japcc.org/conference/.

In closing, I hope you were inspired by the reading and that it serves as a call to action as we collectively strive for the positive transformation of NATO Air and Space Power. We hope that by exposing our readers to a mix of ideas and opinions the collection of papers will be a catalyst for debate that will help shape the future of NATO Air and Space Power. There is much work to be done to ensure NATO can respond at the speed of relevance to deliver Air and Space Power in support of its operations. Your thoughts, insights and perspectives on these topics are welcome and encouraged as an essential element of our discussion.

I sincerely hope to see you this fall in Essen!

Klaus Habersetzer
Lieutenant General, GE AF
Executive Director, JAPCC

Conference Itinerary

As of May 2021

7 September 2021
Icebreaker and Industry Showcase

8 September 2021
Inaugural Session with JAPCC Director's Opening Address
Keynote Speech
Panel 1: Policy and Strategy
Director's Luncheon and Lunch Buffet
Panel 2: Leveraging Emerging Technologies
Panel 3: Dynamic C2 Synchronized Across Domains
Director and VIP Tour of Industry Showcases
Networking Dinner and Industry Showcase

9 September 2021
Keynote Speech
Panel 4: Superiority in the Electromagnetic Spectrum
Lunch Buffet
Panel 5: NATO Space
Wrap-up and Director's Closing Remarks

Joint Air Power Competence Centre
von-Seydlitz-Kaserne | Römerstraße 140 | 47546 Kalkar (Germany)
Visit us in the web:
www.japcc.org