



Transforming Joint Air and Space Power **The Journal of the JAPCC**



Edition 33, Winter 2021

PAGE 6

Excellence in Joint
Air and Space Power
Director's Reflection

PAGE 42

Possibilities and Limits
of a C2 (R)Evolution

PAGE 62

Space Domain:
A Global Vision

ALONE WE'RE TOUGH. TOGETHER UNBEATABLE.



WE MAKE IT FLY

European air sovereignty will prevail thanks to the Future Combat Air System. At its heart is the Air Combat Cloud. By combining platform capabilities, it makes any military operation more powerful than the sum of its parts. Developed by Airbus and its European industrial partners, it means a stronger Europe ready to face any threat independently.

Connectivity. We make it fly.

It is a great honour to introduce myself as the new editor of the Journal of the JAPCC, and as the newly appointed Assistant Director of the JAPCC. The role of editor is a significant responsibility and I am excited about the future of the journal and committed to helping continue the impressive trajectory it has established over the past 16 years.

A special thanks to our contributing authors starting with our Director, General Harrigian, for what will be his final piece as JAPCC Director. General Harrigian highlights the actions and adaptations undertaken in the Air and Space domains to maintain a competitive edge in the face of the rapidly advancing threats and technology. Continuing under the heading, 'Leadership Perspective', Lieutenant General Luyt, outlines the RNLAF's ongoing process to become a 5th Generation Air Force and emphasizes the crucial role played by the dedicated innovative and transformative units.

The 'Transformation & Capabilities' section unfolds with the article '25 Years of Integrated Air and Missile Defence Training' describing the evolution of the JPOW exercise series experimenting and incorporating more and more assets and players along with transitioning from TMD to IAMD. 'Beyond SEAD' brings into focus the encompassing JADO concept and how the employment of joint capabilities, in a layered approach, can be useful in unlocking the A2/AD problem. 'Air-Land Integration – Bridging the Gaps in Joint with Force Education and Training' builds on a previous article published in edition 30 and brings to surface the need for properly trained personnel to achieve effective joint ALL and interoperability. The following article, 'Defending Space in and through Cyberspace' emphasizes the importance of effectively addressing all cyber concerns and challenges for the protection of space assets. The 'Possibilities and Limits of

a C2 (R)Evolution' article explains how new technological achievements should drive the need for new C2 constructs and exemplifies with instances from the SBAMD realm. Moving further, the 'Responsive Space for NATO Operations – Part 3' article is the concluding piece of the series published in editions 31 and 32. 'Potential Game Changer for Close Air Support' then explores how an enhanced UAS role in contested environments can deliver timely and responsive CAS for operations.

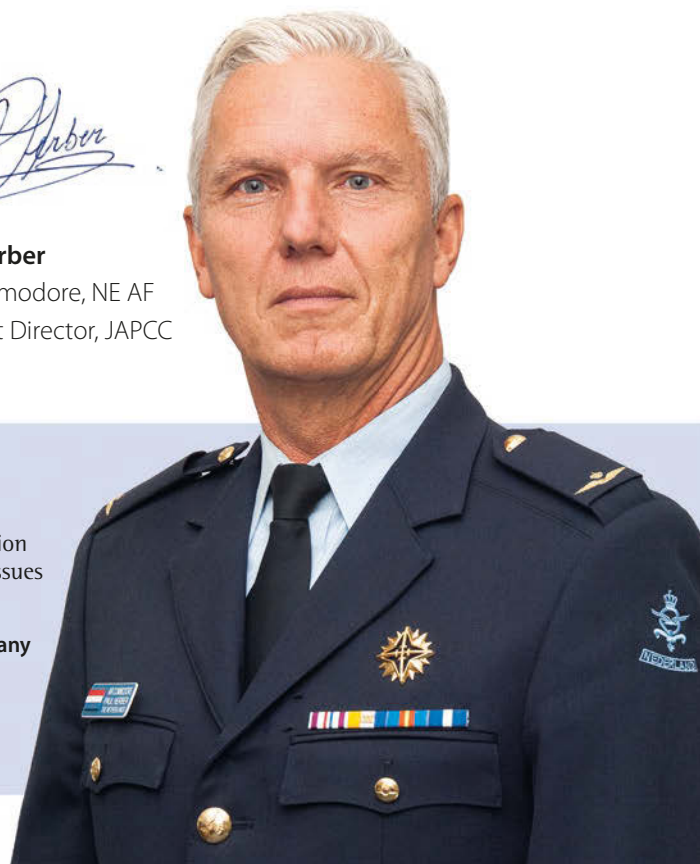
Advancing to the 'Viewpoints' section, the article 'Space Domain: A Global Vision' brings forward the need to increase resiliency and survivability of our space assets. 'Meeting the Needs of Future Warfare' addresses JAPCC's support to the NATO training and exercise endeavour. Concluding this section, the article 'To Be or Not to Be Classified' advocates for a releasable to the public version of the Space Policy. Finally, under the 'Out of the Box' section, 'The TLP and the Pace of Change' article deals with the organization's most current challenges.

Thank you for taking the time to read this edition of our Journal. We hope you will find it informative and stimulating and we greatly appreciate any feedback, thoughts, or ideas you may wish to share. I encourage you to reach out to us via our website at www.japcc.org, like us on LinkedIn or Twitter, or send us an email to contact@japcc.org.



Paul Herber

Air Commodore, NE AF
Assistant Director, JAPCC



The Journal of the JAPCC welcomes unsolicited manuscripts.
Please e-mail submissions to: contact@japcc.org

We encourage comments on the articles in order to promote discussion concerning Air and Space Power. Current and past JAPCC Journal issues can be downloaded from www.japcc.org/journals

The Journal of the JAPCC Römerstraße 140 | D-47546 Kalkar | Germany

Follow us on Social Media





36



24



6

Table of Contents

Leadership Perspective

- 6 Excellence in Joint Air and Space Power
Director's Reflection
- 11 Transforming the RNLAf into a
5th Generation Air Force: Just Doing It!

Transformation & Capabilities

- 17 25 Years of Integrated Air and
Missile Defence Training
*Sharpening and Sharing Knowledge
to Prepare for the Future*
- 24 Beyond SEAD
*Synchronizing Joint Effects to Combat
an A2/AD Threat*
- 30 Air-Land Integration –
Bridging the Gaps in Joint with
Force Education and Training
*Practical Solutions for Air-Land
Interoperability in NATO*
- 36 Defending Space in and
through Cyberspace
A Fragile Stability in Space

- 42 Possibilities and Limits
of a C2 (R)Evolution
- 49 Responsive Space for
NATO Operations – Part 3
- 55 Potential Game Changer
for Close Air Support
*Enhancing UAS Role in Contested
Environments*

Viewpoints

- 62 Space Domain:
A Global Vision
- 68 Meeting the Needs of Future Warfare
*The JAPCC's Experience as a Provider of an
Opposing Forces (OPFOR) Element for
NATO Exercises*
- 74 To Be or Not to Be Classified
*Why Over-Classified Documents Make
NATO's Life Harder: The Overarching
Space Policy as a Prominent Example*

Out of the Box

- 79 The TLP and the Pace of Change
TLP Challenges and Strategy



Copyrights

Front Cover: Special Forces Group: © US Army, Sgt. Steven Lewis; AWAC: © US Air Force, Percy G. Jones; Aircraft Carrier: © US Navy, MC 2nd Class Paul L. Archer; Launch: © ESA-CNES-ARIANESPACE/Optique Vidéo du CSG; Communication Waves: © 2018 backUp/Shutterstock.com; Galaxy/Sky: © Sugrit – stock.adobe.com

Ad 6: © US Air Force, Staff Sgt. Alexander Cook

Ad 24: © US Army

Ad 30: © US Air Force, Senior Airman Milton Hamilton

Ad 36: © NASA/JPL-Caltech

Ad 55: © TU Air Force, Ozkan Uner

Inside the JAPCC

86 Joint Air and Space Power Conference 2021
Delivering NATO Air and Space Power at the Speed of Relevance

JAPCC Hosts 8th Annual Joint Air and Space Power Network Meeting
NATO and European Air and Space Future Challenges

JAPCC Hosts the NATO Air Operations Working Group

2021 Maritime Air Coordination Conference

Handover Ceremony of the Assistant Director Post in JAPCC
A New Era with New Challenges!

Book Reviews

90 'Zero-Sum Victory'
'Airpower Reborn'

Imprint:

**Transforming Joint Air & Space Power:
The Journal of the JAPCC**

Director

Joint Air Power Competence Centre

Gen Jeffrey L. Harrigian

Executive Director

Joint Air Power Competence Centre

Lt Gen Thorsten Poschwatta

Editor

Air Cdre Paul Herber

Assistant Editor

Lt Col Ciprian Teletin

Production and Advertising Manager

Mr Simon J. Ingram

Editorial Review Team

Col Matthew Willis, Col Michael Adams,
Lt Col Isaiah Oppelaar, Mr Adam T. Jux

Purpose

The JAPCC Journal aims to serve as a forum for the presentation and stimulation of innovative thinking about strategic, operational and tactical aspects of Joint Air and Space Power. These include capability development, concept and doctrine, techniques and procedures, interoperability, exercise and training, force structure and readiness, etc.

Disclaimer

The views and opinions expressed or implied in the JAPCC Journal are those of the authors concerned and should not be construed as carrying the official sanction of NATO.

Terms of Use – Alteration, Notices

This Journal may be reproduced for instruction, reference or analysis under the following conditions: 1. You may not use this work for any commercial purposes, nor may it be used as supporting content for any commercial product or service. 2. You may not alter, transform, or build upon this work. 3. All copies of this work must display the original copyright notice and website address. 4. A complete reference citing the original work must include the organization, author's name and publication title. 5. Any online reproduction must also provide a link to the JAPCC website www.japcc.org, and the JAPCC requests a courtesy line.

The JAPCC Journal made use of other parties' intellectual property in compliance with their terms of use, taking reasonable care to include originator source and copyright information in the appropriate credit line. The originator's terms of use guide the re-use of such material. To obtain permission to reproduce such material, please contact the copyright owner of such material rather than the JAPCC.

In case of doubt, please contact us.

Denotes images digitally manipulated



Excellence in Joint Air and Space Power

Director's Reflection

By General Jeffrey L. Harrigian, US Air Force, Director JAPCC

The last three years presented a dynamic and challenging strategic environment to the North Atlantic Treaty Organization, its Allies and partners across the globe. Looking back to where we started this journey in 2019, we have significantly shifted into an era of fierce strategic global competition where our competitors challenge our norms, test our commitment to our Allies and the international rules-based order, and expose us to rapidly advancing threats and technology.

Throughout these challenges, our collective Air and Space Power team, comprised of the Joint Air Power Competence Centre (JAPCC), Allied Air Command (AIRCOM), and the Nations' Air and Space Forces, have consistently delivered effects for the Alliance: 24/7 Air Policing and Ballistic Missile Defence Mission; adopting and operationalizing the Deterrence and Defence of the Euro-Atlantic Area concept; and championing a collective approach to change and shape the future.



© US Air Force, Staff Sgt. Alexander Cook

These enormous and essential tasks continue to move forward due to the dedication, perseverance, and ingenuity of our amazing people.

The Alliance demonstrated a shift in strategic focus during 2019. In response to acknowledging Russia as a strategic competitor with activities across all domains, NATO implemented a series of work strands that focused on reinforcing the commitment to collective defence and modernizing our approach to the adversary. A seminal NATO Military Strategy set the groundwork for maintaining a credible and effective deterrence and defence. Core to success in these areas is a simplified Command and Control (C2) structure – executable, repeatable, and understood. Subject matter experts from AIRCOM and the JAPCC supported the creation of a Joint C2 Concept of Operations and crafted an Air C2 Concept of Operations that provides flexibility, adaptability, and resilient control with a theatre-wide approach utilizing supported and supporting relationships. Proven in

multiple joint exercises since 2019, this construct continues to be the template for component C2 across the Alliance.

NATO continued to adapt by recognizing the need to officially declare Space as an operational domain in December of 2019. Approximately ten months later, in October of 2020, the NATO Space Centre was created to support NATO activities and operations, increase NATO Space Domain awareness, and help protect Allied Space systems by sharing information. Coordination with nations in the Space domain is a critical mission as civilian, military, and commercial organizations increasingly depend on Space capabilities for our safety and security. Space domain barriers to entry continue to diminish. Commercial companies such as Boeing, SpaceX, Virgin Galactic, and Blue Origin provide low-cost logistical support for nations, industry (banking, agriculture, communications), and even leisure travel. Based on this growth, we must prepare for fierce competition in Space.

Consequently, NATO is committed to ensuring free and open access to the Space commons, focusing on increased Alliance Space domain awareness, promoting adherence to internationally recognized norms, and deterring actions that would lead to militarization of Space. Additionally, the advent of commercial leisure travel in Space brings a literal new dimension to protection and security of the extraterrestrial and beyond.



To support the Space domain, NATO approved a new Space Centre of Excellence, based in Toulouse, France. During the stand-up and transition period, the JAPCC will continue to provide space-related articles, research, and advice and looks forward to supporting the new Space Centre of Excellence in the future.

Outside of the advent of the Space domain, the year 2020 brought its unique set of challenges. A pandemic gripped the world in early 2020. The COVID-19 virus exploded across the globe, hindering the world economy, altering personal and professional interactions, and testing the strength and fabric of the NATO Alliance. However, even with these uncertain pressures, Air Policing activities remained stalwart and consistent, executing a record number of air intercepts in 2020. With the activation of Rapid Air Mobility processes, Airmen facilitated short notice movements of medical supplies throughout their Area of Responsibility (AOR). Innovative operations enabled continued progress on essential projects, large-scale training and exercises, and continued readiness of the multinational force. In fact, the Alliance's human element – its people, its backbone – adapted and overcame the struggles with perseverance and innovative thinking ensuring the health crisis did not turn into a security crisis while continuing to deliver 24/7 Air and Space Power to the Alliance.

The concept for Deterrence and Defence of the Euro-Atlantic Area (DDA) shifted focus to address a 360-degree threat across the entirety of the Supreme Allied Commander Europe (SACEUR) AOR. The refined C2 structures execute supported and supporting relationships that rely on high levels of trust and confidence between commanders, in order to provide effects with constrained resources. We drew support from across the Alliance, nurtured relationships with partners, and solidified the all-domain connective tissue through exercises such as Steadfast Jupiter and Ramstein Ambition.

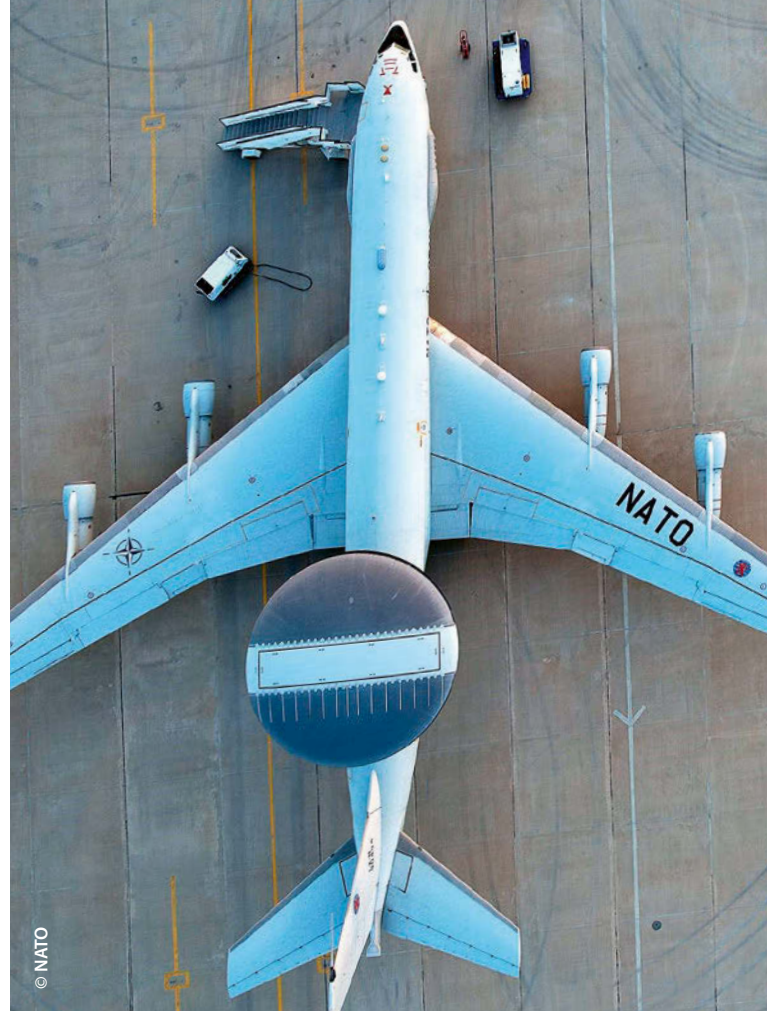
Furthermore, effective deterrence requires coherent national input. In an effort to align national activities, the air component increased collaboration with the maritime component to create repeatable, operational training opportunities that span multiple domains (AIRCOM/MARCOM playbooks). These events test the connective tissues of joint C2, strengthens national and

Alliance relationships, and builds a more refined and competent deterrence force. Similarly, we continued to educate the collective Air and Space community with publications and reviews such as the *'A Comprehensive Approach to Countering Unmanned Aircraft Systems'* book and the JAPCC Journals, to study topics such as Joint All-Domain Operations and to connect via the in-person JAPCC Conference, the NATO Air Chiefs Symposium, and the Partner Air Chiefs Conference. These efforts consistently brought together Air and Space leaders to build relationships and strengthen the collective commitment to maintaining peace and stability.

Throughout 2021, we continued to develop and integrate new Air and Space capabilities. The 5th generation aircraft are integrating into numerous NATO Allied Air Forces' inventories and drive nations to normalize tactics, techniques, and procedures for 4th and 5th generation aircraft integration. These aircraft are essential to the deterrence and defence of the Euro-Atlantic Area and nations have executed Air Policing in the North Atlantic, Baltic, and Mediterranean areas. Moreover, 5th generation subject matter experts have been incorporated in HQ AIRCOM Joint Force Air Component staff, providing knowledge and experience essential to our planning and daily operations.

As an Alliance, we must leverage the technological capabilities provided by these stealth aircraft to increase connectivity and our situational awareness throughout SACEUR's Area of Operations through multinational training such as Atlantic Trident and Falcon Strike. We must also recognize that a single platform by itself cannot meet the full potential of its capabilities, but instead must contribute to a system of systems that connects our Allies and partners through a shared common operational picture. Our most effective force will only be realized with national input and enhanced communications sharing.

In late summer of 2021, the world witnessed the end of a decades-long war in Afghanistan. In a massive, short-notice airlift operation, the power and capability of air mobility was demonstrated on a world stage. In conjunction with multinational efforts, NATO's Operation Allied Solace accomplished what is likely the most significant airlift operation of the 21st century.



The success was only accomplished through the close cooperation and integration of our allies and partners across the globe. Our aircrews demonstrated that flexibility is the key to Air Power and, even in a stressful and discordant environment, underlined the commitment, determination, and courage of NATO's men and women. This event reaffirmed the Alliance's commitment to our shared values, considering the human side of conflict and providing dedicated military and civilian support to the families airlifted to safety. As we all know, we are stronger together and I am extremely proud of the efforts of our team.

The Alliance continued to further align its focus with a near-term operational perspective in SACEUR's AOR Wide Strategic Plan and a long-term perspective of how to think, act, organize, and adapt in the NATO Warfighting Capstone Concept. This alignment is necessary to address technology advances that can threaten large population centres and put the security of Alliance members at risk. The use of grey zone tactics to blur the lines between outright acts of aggression and peaceful competition demands innovative solutions. Therefore, we must embrace change,

‘... aircrews demonstrated that flexibility is the key to Air Power and, even in a stressful and discordant environment, underlined the commitment, determination, and courage of NATO’s men and women.’

remain aligned with our Allies and partners, and ensure the highest levels of force readiness to be able to win in deterring our adversaries.

Looking forward to 2022 and the future, the Air Component will continue to deliver joint effects while recognizing challenges, creating innovative solutions, and adapting to the shifting environment. These efforts will expand our competitive edge into the future and remain fundamental to sustained success. Effective C2 will rely on timely and accurate indications and warnings. Cutting-edge technologies such as cloud computing and artificial intelligence will be integral to Alliance intelligence, C2, and delegated authorities. To remain both strategically relevant and tactically efficient demands an ability to make decisions at speed. Joint All-Domain Operations and NATO’s Alliance Future Surveillance and Control require reliable information that is accessible to the

right decision-makers at the right time, ultimately providing an undeniable advantage in information, awareness, and decision-making. The Air and Space domains recognize that open architecture systems which embed coders with warfighters enable software enhancements that meet and likewise challenge the adversary. We must lead the joint force in breaking free from our preconceived notions to be ready for the next conflict.

Reflecting on my time as Commander Allied Air Command, no matter how much the world has changed, I am encouraged to see that the Alliance remains strong, committed to its Allies, and prepared to deter and defend. I am very proud of the role the JAPCC played in fostering strategic thinking and providing the Alliance with extremely valuable Air and Space deliverables again and again. As the oldest and notably the highest producing Centre of Excellence, the JAPCC has and will continue to support the Air and Space Power community as it continues to meet the call of providing air and space power, at any time and any place and under any conditions. Lastly, I must note that the continued successes of NATO Allied Air Command are built upon the shoulders of our individual Airmen. The future of the Air and Space domains is in great hands ... ●

General Jeffrey L. Harrigian

is the Commander of the Allied Air Command, Commander of the US Air Forces in Europe, Commander of the US Air Forces Africa, and Director of the Joint Air Power Competence Centre. He is responsible for Air Force activities in an area covering more than 19 million square miles. As Commander of the Allied Air Command, General Harrigian is responsible to the Supreme Allied Commander Europe for the Air and Missile Defence of NATO Alliance member nations during peacetime operations. Furthermore, in the event of a joint NATO operation, he is the responsible commander of the Air Component.

General Harrigian is a graduate of the US Air Force Academy. He has served in a variety of assignments, including Commander of the US Air Forces Central Command, Combined Force Air Component Commander, US Central Command; Deputy Director for Strategy, Plans and Assessments, US Forces-Iraq; and Chief of the Joint Exercise Division at NATO’s Joint Warfare Centre, Stavanger, Norway. He has flown combat missions in support of operations Just Cause, Desert Storm and Inherent Resolve.

General Harrigian is a command pilot with more than 4,100 hours in the F-22, F-15C, A/OA-37 and MQ-1 aircraft.





Transforming the RNLAF into a 5th Generation Air Force: Just Doing It!

By Lieutenant General Dennis Luyt, Commander, Royal Netherlands Air Force

Introduction

The world is changing rapidly. The geopolitical landscape is transforming as a result of the strategic competition among existing, emerging, and revisionist powers. Simultaneously, these powers are developing emerging technologies, such as artificial intelligence, quantum computing, and hypersonic missiles at an incredibly rapid pace. Our societies are more connected

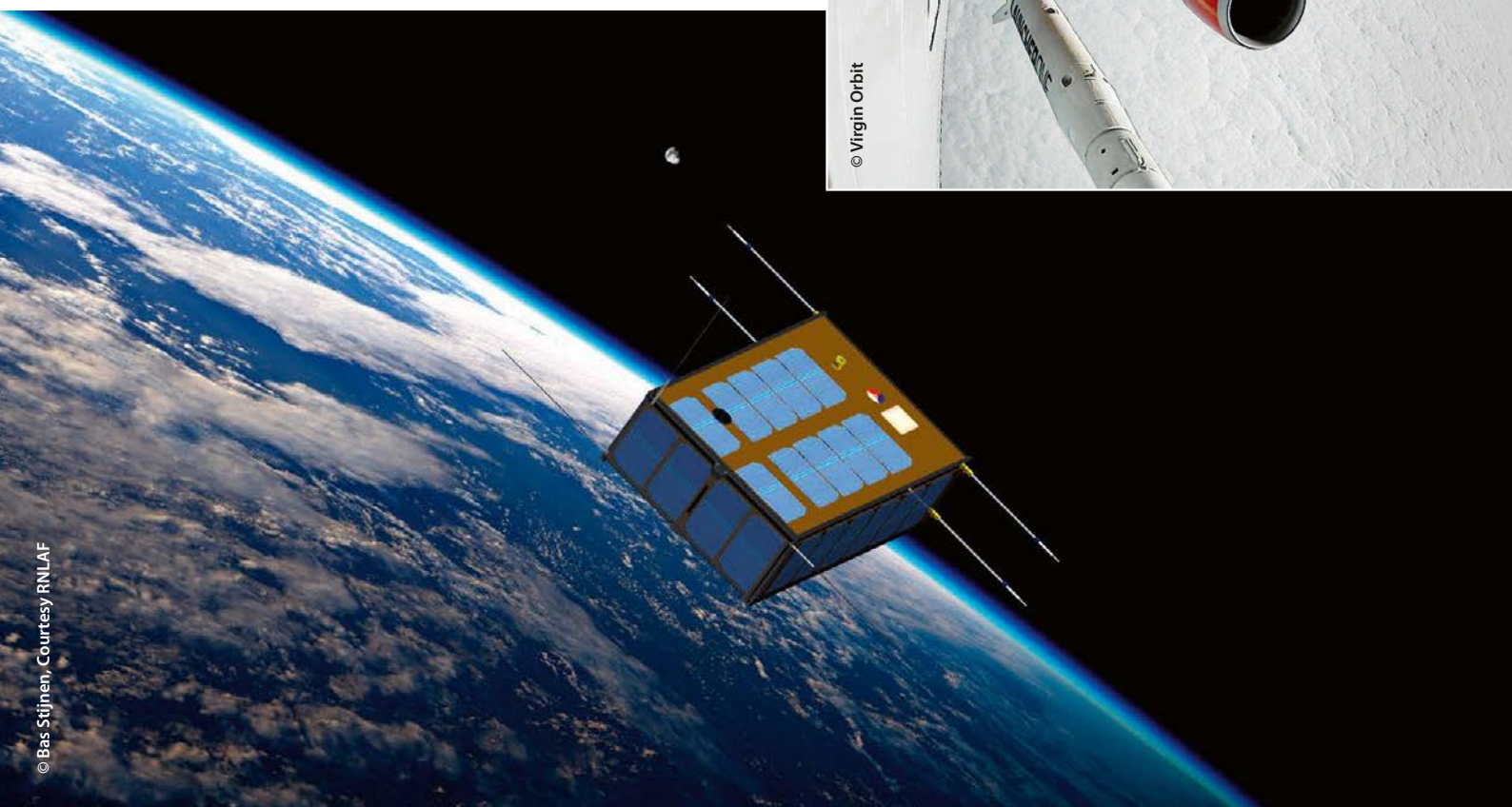
through our smartphones, smart homes, and the internet of things. The growing world population is struggling to comprehend and overcome the challenges of climate change and global pandemics, resulting in an economy under pressure from both events. These trends and developments impact our armed forces in their efforts to stay relevant in safeguarding peace and security and making the necessary changes to organizations, capabilities, and operational concepts.

In this volatile, uncertain, complex, and ambiguous context, the Royal Netherlands Air Force (RNLAF) is transforming into a 5th Generation Air Force. Since we launched our '*5th Generation Air Force*' vision in 2017, the RNLAF has incorporated a number of new weapon systems: our new Chinook F/CAAS-helicopters, the multinational A330 MRTT, the MQ-9 Reaper, and the F-35 Lightning II. Perhaps less visible, but certainly not less important, we have been transforming our organization, including how we train and exercise, to prepare for Joint All-Domain Operations (JADO). Finally, we have put information, data science, and software at the core of our efforts to improve our processes to fly, fight, and win more effectively and more safely. This article will highlight some of our 'lighthouse projects'¹ to illustrate the challenges we had to overcome and the solutions we were able to find. It will first look at the new possibilities that 5th generation capabilities offer, particularly sensors and connectivity. Next, it will explain innovative ways of implementing the required changes. Finally, the article will provide an insight into some of the innovative

and transformative units that are leading the way toward operationalizing our '*5th Generation Air Force*' vision: the Data Science Cell, the Space Security Centre, the Cyber Warfare Team and the F-35 Operational Test and Evaluation (OT&E) Unit. The article will conclude by drawing conclusions and providing some key takeaways.

New Capabilities Supporting the Joint All-Domain Fight

The 5th generation capabilities are mainly about employing 'next-level' weapons systems to speed up our effects-cycle so we 'outpace' and 'outsmart' an opponent. It is also about keeping the technological edge over potential adversaries. Leading-edge technologies



are applied to combine sensors with kinetic and non-kinetic effectors resulting in improved connectivity and survivability. The F-35 is clearly the centrepiece of our 5th generation air combat capability, but other new weapon systems like the MQ-9 and our new AH-64E are also part of the bedrock that underpins a next-level Air Force. The F-35 combines low observability with a sensor suite that is unmatched by any 4th generation fighter aircraft. On top of that, stand-off capabilities enable us to exploit altitude, speed, and range to our advantage. Furthermore, the F-35 brings new maintenance and logistics concepts to maximize mission availability. Clearly, 5th generation capabilities bring to bear the ability to operate near and through Anti-Access/Area Denial (A2/AD) regions that some of the revisionist powers tend to deploy. As advanced as the aircraft and its systems may be, to prevail in tomorrow's combat missions, the main aim is to overwhelm potential adversaries with challenges and to get inside their Observe-Orient-Decide-Act (OODA) loop. Information dominance enables decision dominance, which is required to deter, defend, and dominate in modern combat. This means that data and information handling are becoming more critical in support of airpower. It is my firm belief that in the upcoming decade software will become as important, if not more important, than hardware. 5th generation capabilities are synonymous with information, are data-driven by design, and are potentially capable of functioning as nodes in a combat cloud. However, that will only happen if we unlock and find ways to share data and information more seamlessly than we are able to do now. As a coalition, we still have some steps to go to make this happen.

Innovate by Doing!

Receiving 5th generation capabilities stresses the importance of what we call an 'operational information backbone'. This federated combat network with layered security connects participants in multiple domains and enables joint all-domain command and control. During the first few years of our transformation, we found that building and experimenting with small parts of this network is more important than



 MQ-9 Reaper: © MCD, Jan Dijkstra;
Drone Operator: © MCD, Jasper Verolme



first designing (and debating) an overall solution. Modus operandi from the digital industry assisted us in digitizing the battlespace and improving our adaptability to rapidly changing threat conditions. The use of Artificial Intelligence (AI) and Robotic Process Automation (RPA) freed up scarce resources (i.e. personnel), particularly in processes that comprise dirty, dull, or dangerous tasks. The newly available resources are necessary to continue to perform operational tasks that require meaningful human control. Therefore, future combat units will have to be resourced with cyber experts, data scientists, and AI-specialists that continuously support the unit in improving its combat effectiveness. These changes cannot happen overnight, but they can begin in small start-up formats at the edges of our organization and in close cooperation with civil partners. These projects are designed to either fail fast or be scaled-up, if successful. It was merely the combination of the inherently pioneering spirit of our Airmen and the cooperation with digital partners that enabled us to stand-up and scale-up the following 5th generation lighthouse units. However, we need to

be realistic about the tempo we can achieve in scaling our innovative efforts. Most of our Air Forces are facing limited budgets which, combined with the limited personnel resources we can dedicate to the innovation of all our other tasks, drives the tempo of our common innovation agendas.

The RNLAF's Lighthouse Units

The Data Science Cell (DSC)

The DSC delivers data-driven, decision-making support products to accelerate and strengthen our transition to the 5th Generation RNLAF. The DSC started in 2017 and groups together a small number of military and civil data science experts. Firstly, the DSC tested and experimented with big data analysis to prove its added value for the RNLAF. This first phase concluded in less than a year and the RNLAF decided to take DSC to the next level and connect it to the operational and maintenance processes. Today the DSC is working on applications in the fields of predictive



flight maintenance planning, long-term readiness planning, human resources analytics, and analysis of imagery from the sensors of 5th generation systems.

The Defence Space Security Center (DSSC)

In response to developments in the geopolitical arena and the lower threshold of access to space capabilities, the RNLAf has started to develop knowledge in the military use of space with the aid of the DSSC. After building capacity for monitoring space weather and developing space situational awareness, we recently launched a small communication satellite named 'BRIK II'. This project was conducted in close cooperation with the Dutch small satellite or SmallSat enterprise and the Royal Aerospace Laboratory (NLR). The launch was contracted to Virgin Orbit, which gave us an opportunity to experiment with Responsive Launch Capability. Furthermore, the dual-use nature of space capabilities offers exciting opportunities to cooperate among European militaries and industries with the aim of improving Europe's strategic autonomy in space. Even though the Ministry of Defence has

not yet issued a formal space policy, the RNLAf is ready to scale up its efforts to develop a national military use of space capability in order to safeguard national and European interests in this new domain. Obviously, we are also building this capability on the foundation of our transatlantic partnership. This is illustrated by our participation in the Responsive Space Capability programme, among other projects.

Cyber Warfare Team

Geopolitical developments have led to strategic competition in cyberspace. Hyper-connected societies have become more vulnerable to threats in the virtual and cognitive domains. Cyber security has become an essential part of any company's or organization's efforts to mitigate the risks of cybercrime and other digital attacks. Modern 5th generation capabilities rely heavily on connectivity and thus have become vulnerable to cyber threats. That is why the RNLAf Cyber Warfare Team currently focusses on defensive and preventive strategies to Cyber Readiness in a two-way approach. Firstly, we educate our personnel on Cyber Awareness and Cyber Security, so our people can function as smart sensors. Secondly, we run risk and vulnerability management (on- and off-base) and central monitoring of our essential digital systems and networks in our Cyber Security Operations Center (CSOC). In addition, offensive cyber and electromagnetic activities are employed in cooperation with the Defence Cyber Command. The Cyber Warfare Team is another example of a typical 5th generation unit that is very small in numbers, but potentially high in impact. This is also in line with the RNLAf motto: '*Parvus Numero Magnus Merito*' (Small in numbers, great in achievements).

F-35 OT&E Squadron

Having received less than half of the initially ordered F-35 fleet, we have been able to reach Initial Operational Capability (IOC) in December of 2021. Even before the delivery of the first aircraft, a small OT&E unit has put significant effort into developing the necessary skills, concepts, and Tactics, Techniques, and Procedures (TTP) required to operate the F-35. This OT&E unit was initially co-located with our United States,

United Kingdom, and Australian partners. This test unit has transferred its results to the first F-35 squadron in the Netherlands. All fields of expertise involved in F-35 operations had to adapt their way of working to the newly available technologies that are incorporated into the operations and maintenance concepts. On the operational side, we have seen a shift in the balance between live flying and simulated training efforts. Not only does the F-35 simulator provide the latest technology in live-virtual-constructive training, but the joint all-domain context also drives the need to simulate more challenging scenarios. On the maintenance side, the system presents fewer challenges in repairing single items, which leads to a more system-oriented approach by the technicians. The traditional three-tiered organization of the maintenance system is becoming obsolete, which requires the maintenance organization to transform itself to meet the new requirements and guarantee the required high levels of serviceability together with commercial partners.

Conclusions and Key Takeaways

The transition of the RNLAF to becoming a 5th Generation Air Force is well underway. Using an innovative approach by starting small, failing fast, and cooperating with digital partners has paid off for a number of

lighthouse units. Apart from procuring and implementing 5th generation capabilities, it has been crucial to focus on transforming the organization and mindset. A large part of this mindset is about learning by doing. We have been able to make huge steps because of this approach. Putting data and software at the core of the transition has proven to be as important as the hardware we operate. Even though the transition is still ongoing, I feel confident that we are on the right track. It makes me proud to see how our women and men apply innovative approaches on a daily basis to make our vision a reality. To sum it up, the key takeaways are:

- 5th generation capabilities open up new ways to meet the challenge of a rapidly evolving threat.
- Software and data drive the effectiveness of our hardware and our weapon systems.
- 5th generation air forces should foster an innovative, pioneering spirit and provide room for failing fast and scaling up at speed.
- Small lighthouse projects – learning by doing – function as accelerators for innovation, cooperation, and results.
- Doing is the new designing! ●

1. 'Lighthouse project' is a term that is used in the NE Armed Forces to identify a project or unit that tests new concepts and demonstrates new capabilities in order to lay the foundation for scaling up and implementing these concepts and capabilities.

Lieutenant General Dennis Luyt

was appointed as Commander of the Royal Netherlands Air Force on 10 June 2016. He started his military career at the Royal Military Academy in 1981. After studying Aircraft Engineering, he attended pilot training at the Euro-NATO Joint Jet Pilot Training (ENJJPT) in the United States in 1985, receiving his wings in December of the same year. In 1986, he received conversion training for the NF-5 at Twente Air Base, followed by conversion training for the F-16 two years later. After this conversion, he was appointed to several positions in operational F-16 units and flew the F-18 as an exchange with the RCAF.

In 2007, following a tour as Military Assistant (MA) to the DCOM Air at ISAF HQ in Afghanistan, he was assigned, in October, to the Integral Plans Branch of the Defence Staff in the rank of Colonel, initially as Head of Project Planning and later Head of Planning Integration. In April 2010, became the Commanding Officer of the Leeuwarden Air Base. On 24 August 2012, was appointed Director of Operations of the Royal Netherlands Air Force, and concurrently promoted to the rank of Air Commodore. Following this appointment, in June 2014, he was promoted to Major General and made Director of Operational Readiness for the Netherlands MoD.





© DGLC

25 Years of Integrated Air and Missile Defence Training

Sharpening and Sharing Knowledge to Prepare for the Future

By Lieutenant Colonel G. W. 'Berry' Pronk, NE AF, JAPCC

Introduction

The Cold War timeframe is often looked upon as a gloomy era; however, it also provided positive things, like military, social, and relative political stability in Western Europe. The end of the Cold War gave impetus to countries to adapt their foreign policies, thus opening up an era of instability right at NATO's eastern borders. In 1990, after the Iraqi

invasion of Kuwait, a US-led coalition started preparing an adequate answer for what was considered Iraqi aggression.¹ During Operation Desert Storm, the United States (US), the Netherlands, and latterly Germany, decided to deploy Surface Based Air and Missile Defence (SBAMD) forces to NATO's border with Iraq, in eastern Turkey. In addition, the US and the Netherlands deployed PATRIOT SBAMD units into Israel.

Operation Desert Storm opened a new era of conceptual thinking regarding the application of military force in a high-tech networked battlefield and perhaps was the first example of a Multi-Domain/Joint All Domain Operation ('MDO/JADO avant la lettre'). The operation presented the possibilities and advantages of networked operations. Theatre Missile Defence (TMD) was a significant part of Operation Desert Storm, and for the countries that owned PATRIOT systems, it became clear what advantages had been put in place. As a result, they managed to connect through tactical datalinks to higher and lateral units and receive valuable data that was not available in a stand-alone configuration. Although modern at the time, this conflict with occasional uncoordinated air and ground operations merely ushered in the interoperability revolution. Participating nations, and even within the countries' different services, found that although you may have the same equipment and datalink protocols, it does not necessarily mean that you have connectivity, let alone interoperability. Big steps still needed to be taken towards establishing Network Centric Warfare.

Interoperability and Interconnectivity

The last decade of the 20th century proved critical for Integrated Air and Missile Defence (IAMD). NATO dismantled its Defensive Counter Air (DCA) belt, comprised

of SBAMD systems and air defence fighters, that had provided comprehensive air defence and had protected NATO's manoeuvre forces at the inner German border during the Cold War, and moved to a more flexible SBAMD cluster defence. At the same time, Command and Control (C2) was improved with the Surface-to-Air Missile/Control and Reporting Centre (SAM/CRC) interface system and air picture sharing in a Common Tactical and Operational Picture, which then became the norm. Shortly after Operation Desert Storm, the US, Germany, and the Netherlands, mainly due to their Theatre Air & Missile Defence cooperation experiences during that operation, started to work on improving their interoperability.² In 1994, the first field trials took place between the Netherlands' Air Force 5th SAM Battalion and the US 69th ADA Brigade, at the time, both were based in Germany. During NATO exercise Dynamic Guard in 1994 (Greece/Turkey area), Netherlands PATRIOT operators and US airmen created the first NATO network with Netherlands, a US Air C2 node (Mobile C2 Element) and an experimental Theatre Missile Defence Cell, equipped with Joint Tactical Ground System³ workstations. These successful tests led to the first full participation and integration of a Netherlands PATRIOT/HAWK battalion in the US exercise Roving Sands in 1995. In addition, it gave access to the Joint Project Optic Cobra TMD exercise, a US Forces Command Theatre Missile Defence live and simulated experiment.

Joint Project Optic Windmill

The above-mentioned initiatives, often flowing bottom-up, were the main drivers for allied interoperability in that era. The lessons learned from Operation Desert



JOINT PROJECT OPTIC WINDMILL '96

Joint Project Optic Windmill '96 (JPOW '96) is the second Central Region Joint Theater Missile Defense (JMTD) exercise, overlaid onto a National exercise of the Royal Netherlands Air Force (RNLAf). JPOW focuses on all aspects (Attack Operations/Counterforce Attack, Active Defense, Passive Defense and Battle Management, Command, Control, Communications, Computers & Intelligence - [BM/C4I]). JPOW '96 provides an unique opportunity validating USEUCOM TMD and NATO's EAD/TMD efforts. Also JPOW '96 provides the opportunity to evaluate the ongoing interconnectivity achievements between the Joint Armed Forces of the United States, Germany and the Netherlands.



PARTICIPANTS

JPOW '96 Participants are

- USEUCOM TMD & SPACE
- AIR SURVEILLANCE TESTBED (AST)



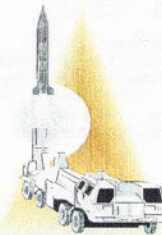
- NATO AIR DEFENSE GROUND ENVIRONMENT
NATO ICAOC 2
NATO E3A NAEW
RNLAf CRC NM
- GROUND BASED AIR DEFENSE
RNLAf MSL GROUP DE PEEL
GAF SAM WING 3 (SAMOC)
GAF SAM WING 2 (SAM GROUP 24)
- FIGHTER/BOMBER A/C
RNLAf F-16
- SEA BASED AIR DEFENSE
RNLAf NAVY

OBJECTIVES JPOW '96

1. Refine Nato, Useucum and National (Prelim) Tactics, Techniques, Procedures and C4I Architectures for Conducting Joint Theater Missile Defense Within Nato's Operational Area of Responsibility.

2. Assess and Document Tactics, Techniques and Procedures, Organization Structures and C4I Systems for Conducting:

- Attack Operations/Counterforce Attack Operations
- Active Defense
- Passive Defense



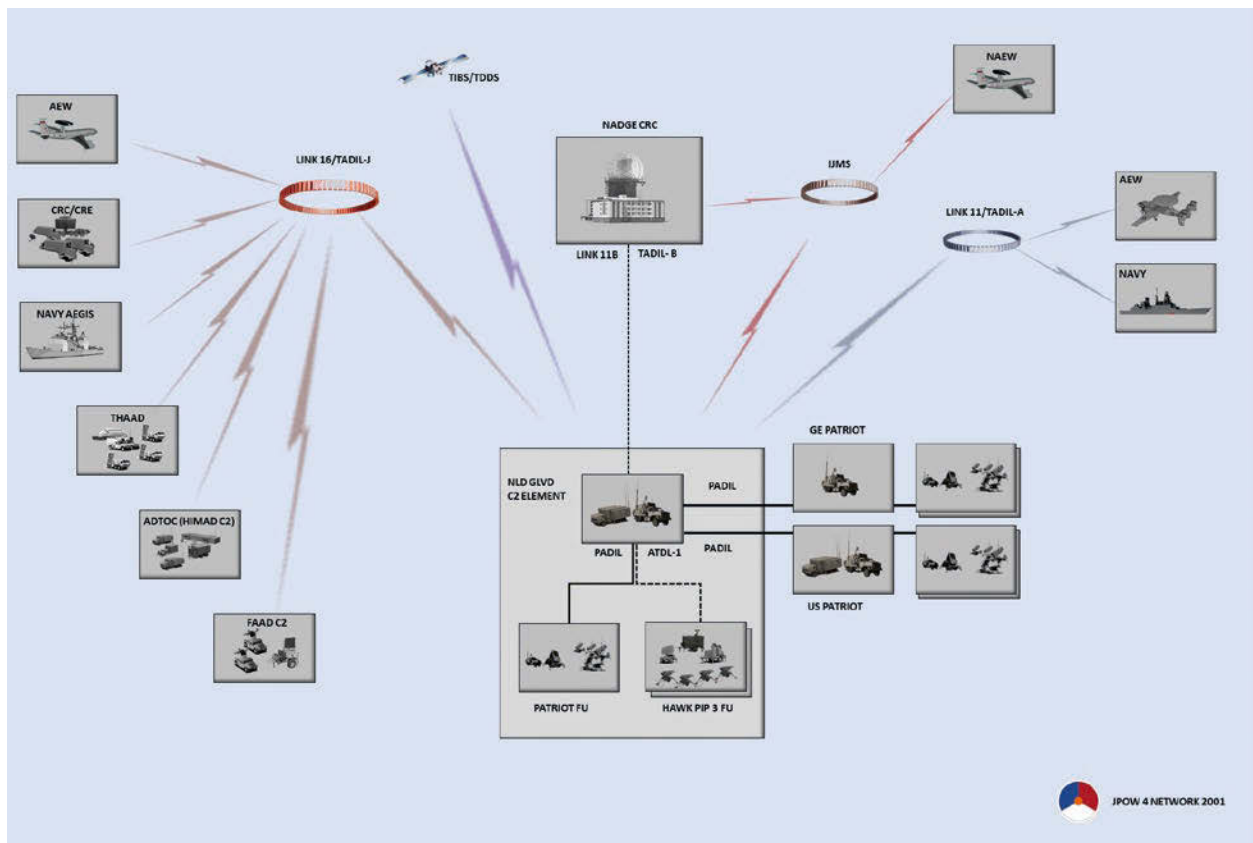
Royal Netherlands Air Force
Directorate of Operations
SAM & Groundoperations Division
SAM/SHORAD Branch
P.O. Box 20703
2500 ES The Hague
Netherlands
Tel: (31)70-3492763 Fax: (31)70-3492726

© RNLAf, Bart van der Graaff

Storm and the lack of sufficient TMD training opportunities in NATO, especially at the tactical level, made it clear that something was missing to properly prepare for future conflicts. The missing element was IAMD training, with an emphasis on **integrated**. As a result, a dedicated team of experts from the Royal Netherlands Air Force, the German Air Force, and US European Command (US EUCOM) took the initiative to organize a small-scale TMD exercise called Joint Project Optic

Windmill (JPOW), complementary to the larger US exercises. The initial goal of this initiative was to bring TMD operations to a lower tactical level, to exercise, and to maximize the interoperability potential between the, at that time, three main PATRIOT users: the US Army, the German Air Force, and the Netherlands Air Force.





The exercise not only provided an excellent training opportunity but also helped to develop procedures on how to connect different communication systems and operate as a networked group. JPOW 1 proved to be a great success and clearly filled a void in the exercise calendar for training in this field. As a result, JPOW became an annually recurring event.

The exercise grew when military doctrine transitioned from Network Centric Warfare towards Network Enabled Capabilities, as the new reference term and subsequently matured swiftly, especially when the US Ballistic Missile Defense Organization (currently, the Missile Defense Agency) became a main sponsor of the exercise and introduced state-of-the-art simulation techniques. Incorporating the CRC capability and NATO's Air Component Command level enabled experimentation with DCA and TMD resource planning. Throughout the years, JPOW evolved and matured from a small-scale tactical-level TMD initiative to a leading IAMD exercise for both the

tactical and operational levels throughout Europe. In 2000, NATO exercise Central Enterprise joined with JPOW and morphed into a unique Air C2 exercise employing live flying and simulated air and missile threats in one scenario. Additionally, JPOW exercises were often used by US units to familiarize themselves with NATO procedures.

The exercise sequels always intend to simulate fighting a battle that is to be expected approximately five to ten years in the future. This time frame enabled experimental systems or capabilities to play in as realistic as possible future scenarios and, whilst doing that, triggering operators to reconsider a future environment in which those experimental systems may have greatest effect. In 2008, at the Bucharest summit, US President G. W. Bush offered the US missile defence capability to NATO.⁴ At that time, the US intended to place ground-based interceptors in Poland and Romania as well as a large X-Band Radar in the Czech Republic. JPOW was the first exercise to provide

a playground to experiment with the C2 of those types of capabilities. The US Strategic Command, Joint Functional Integrated Component Command Integrated Missile Defense, joined up with European planners to experiment with a Missile Defence Coordination Cell (MDCC) in the autumn of 2008. At that time, JPOW took place combined with the US homeland defence exercise Joint Project Optic Alliance. The experimental European MDCC provided coordination in the European theatre and liaised with the US homeland defence forces. MDCC further evolved during the following JPOW exercises and laid the basis for the current NATO Ballistic Missile Defence Operation Centre.

The JPOW Concept

JPOW is an exercise that can facilitate adequate room for experimentation and enable great training possibilities, shaped for optimal knowledge enrichment. Each sequel is set-up based on a previously proven concept, providing a stakeholder-created scenario coalescing all participants' exercise objectives and embedding a thorough analysis of all operators' actions. The analysis takes place in the daily debriefings at the tactical and operational levels. Proper employment of this feedback process and the direct application of lessons learned into the following day's exercise with a slightly adapted scenario, if needed, enabled a steep learning curve and so-called 'knowledge cross-fertilization' amongst the participants. This set-up is unique to NATO.

JPOW is a Computer-Aided Exercise, and its network setup enables participation from De Peel Airbase in the Netherlands or play distributed via a Combined Federated Battle Laboratories⁵ network connection from home locations. Participants have the possibility to play with their real weapon systems (Hardware In The Loop), connect via a simulator or even play with a computer model (Constructive Simulation). The latter applies more in the case of Doctrine, Techniques, Tactics and Procedures (DTTP) development. All are embedded in one exercise network loop, along with simulated air and missile threats. As mentioned, there have even been JPOW editions that paired with live air operations, exercising specific procedures such as

time-sensitive targeting. The exercise also contains an academic phase to prepare the participants, particularly underlining exercise novelties.

The JPOW exercise network, like actual operations, can be set-up at any location on earth. The JPOW project office experimented with this set-up by playing from locations other than De Peel Airbase, like Sigonella Naval Air Station in 2001 and NATO Missile Firing Installations in 2004 and 2006. The latter sets enabled JPOW to be combined with a live firing phase. Although these out of region JPOW exercises were extremely challenging and innovative, at the same time, they put a lot more stress on the ever-dwindling IAMD community.

Concept Development and Experimentation

Some particular 'required circumstances' cannot be accommodated in a realistic scenario and require an artificial storyline/setting. The exercise can facilitate these requirements through the Concept Development and Experimentation (CD&E) phase. JPOW distinguishes itself from other exercises by including a CD&E phase in the overall exercise set-up. This segment, which normally precedes the execution phase, offers participants the unique opportunity to demonstrate, practice, evaluate, and validate different IAMD programmes and concepts. DTTP can be developed, tested, validated, improved, and re-tested in a test-bed environment. NATO, partner nations, and NATO agencies and organizations make extensive use of this CD&E capability. During the latest editions of JPOW, there were four daily experimental lanes (different scenarios) performed in parallel. The possibility of implementing the lessons identified from the CD&E phase during exercise execution allows for immediate feedback and subsequently leads to improved learning opportunities.

Connecting with New Partners

In 2002, NATO began enhanced cooperation with the Russian Federation (RF) establishing a new body, the NATO-Russia Council (NRC),⁶ henceforth NATO being

'committed to making an effective forum for consensus-building, consultations, joint decisions and joint actions'. One of the projects residing under the NRC was TMD, which has turned out to be one of the more promising fields of cooperation.⁷ A delegation of the RF armed forces visited JPOW in 2004 and were impressed by the exercise. In 2005, a JPOW crew supported and facilitated the first European-based NATO-Russia TMD exercise at De Peel Airbase. JPOW personnel also supported subsequent events in Russia. Due to changes in the geopolitical setting, the NRC TMD project slowed down and finally went dormant in 2012.

The change of the overall security situation due to RF posturing attracted the interest of two NATO partner nations, Finland and Sweden, for increased participation in JPOW. The integration of partner nations brings new challenges, like their integration in real time operations. Military/Industrial Foreign Disclosure restrictions, prohibiting access to NATO SECRET networks, have led to the creation of a filtered/parallel network that has been used and improved since JPOW 17 and has enhanced NATO partner integration.

From the Phoenix and Beyond (2017–2021)

In 2012, the Netherlands PATRIOT units, along with German and US SBAMD units, deployed yet again to NATO's south-eastern border.⁸ JPOW being an exercise highly dependent on the support of the hosting Netherlands Joint SBAMD Command, saw the deployment have a significant impact on the manning available for exercise preparation. It must be considered that nearly all exercise control groups are manned by soldiers doing the exercise preparations, in addition to their normal jobs. The upshot was that in 2013 only a small-scale exercise could be held, subsequently proving the infeasibility of continuing the standard JPOW effort.

After the two-year deployment, the equipment went into an extensive and much-needed maintenance period. It was not until 2016 that a small-scale, mainly German/Netherlands version, called 'Constructive Optic



Windmill', was organized to enable a renaissance in the specific JPOW expertise development. Not surprisingly, the phoenix was chosen as the crest for JPOW 2017.

The challenge was to help JPOW rise again from the ashes and get back on its flight path. In 2010, JPOW had close to 2,000 participants from ten NATO nations and entities; playing either from De Peel Airbase or their home locations, ranging from Rome to El Paso and numerous other places worldwide. The 2017 version was a great comeback with the involvement of over a dozen NATO and partner nations, the vast majority participating from De Peel Airbase.

Since 2019, a Combat Enhancement Training/Force Integration Training (CET/FIT) phase was added to the JPOW schedule. Consequently, it enabled better integration of forces from outside the NATO theatre while leading to a better focus on the scenario and settings for all players. At the same time this minimized the loss of playing time due to the unfamiliarity usually experienced during the first days of the exercise. In 2021, JPOW was intertwined with the NATO exercise Steadfast Armour. Although hampered by COVID-19, the 2021 version proceeded with great success, making maximum use of the distributed option that JPOW has to offer.



© DGLC

Currently, JPOW is a German/Netherlands-led exercise that enjoys strong support from US EUCOM, taking place every two years. JPOW has already proven to be a valuable tool in supporting NATO air operations by improving planning and C2 procedures throughout the domain of IAMD. Forged by corresponding IAMD stakeholders, JPOW offers important training opportunities and consistently reflects relevant IAMD issues. The combination of academics, a flexible CD&E, and CET/FIT phases to the actual exercise construct has proven highly effective. NATO regularly expresses its appreciation for JPOW, particularly for its flexible exercise set-up enabling the validation and testing of new ideas and concepts. A considerable part of NATO's

IAMD procedures, as well as parts of its current command structure, were developed and are evaluated during JPOW exercises.

The JPOW exercise is constantly adapting to the changing security environment and is always trying to stay ahead of changes in this arena. This bottom-up developed exercise will continue to remain an important cornerstone for NATO IAMD training. ●

ACKNOWLEDGEMENT

This article is dedicated to:

**Lieutenant Colonel (ret.) RNLAF
Bart van der Graaff**

*Thank you for offering your valuable advice
and warm comradeship.*

1. United Nations Security Council Resolution 678, adopted on 29 November 1990, after reaffirming resolutions 660, 661, 662, 664, 665, 666, 667, 669, 670, 674 and 677 (all in 1990), the Council noted that despite all the United Nations efforts, Iraq continued to defy the Security Council.
2. Maj Gorter & Kap van der Graaff, 'Interoperabiliteit, modewoord of force multiplier' Militaire Spectator JRG 170 6-2001.
3. JTACS, <https://asc.army.mil/web/portfolio-item/joint-tactical-ground-station-jtacs/> (accessed 14 April 2021).
4. CRS Report for Congress, <https://fas.org/sgp/crs/row/RS22847.pdf> (accessed 14 April 2021).
5. CFBL, <https://www.ncia.nato.int/about-us/newsroom/video-enabling-interoperability-a-short-overview-of-cfblnet.html> (accessed 27 September 2021).
6. NATO Russia Council, <https://www.nato.int/nrc-website/en/about/index.html> (accessed 14 April 2021).
7. NATO-Russia TMD cooperation, <https://www.armscontrol.org/act/2003-06/nato-russia-tmd-cooperation-new-phase> (accessed 14 April 2021).
8. <https://www.hln.be/buitenland/nederland-stuurt-patriot-raketten-naar-turkije~a002dd68/?referrer=https://www.google.com/>, <https://www.hln.be/default/duitsland-stuurt-patriot-afweerraketten-naar-turkije~a3699466/> (accessed 14 April 2021).

Lieutenant Colonel G. W. 'Berry' Pronk

has served for over 40 years in the Royal Netherlands armed forces and has completed operational tours during operations Desert Storm, NATO Display Deterrence (US Operation Iraqi Freedom) and in SFOR, former Yugoslavia. He served in various national command and training positions, in the realm of Surface Based Air Defence and Missile Defence, as well as staff positions at the Royal Netherlands Air Force Command and The Royal Netherlands Army Command. Internationally, he served at the former HQ Extended Air Defence Task Force (with US Army and German Air Force) and at the German Air Force Forces Command, as well as Section Chief Air Operations at J3, NATO SHAPE. Currently, the author holds the Subject Matter Expert position for Surface Based Air and Missile Defence at the Joint Air Power Competence Centre in Kalkar, Germany.





Beyond SEAD

Synchronizing Joint Effects to Combat an A2/AD Threat

By Squadron Leader David Tucker, UK AF, CAOC-T

By Major Charilaos Nikou, GR AF, JAPCC

Introduction

In 'The History of the Peloponnesian War', the ancient Greek philosopher-historian Thucydides charted the war events which took place between Athens and Sparta (431–404 BC). One of the most significant parts is the 'Melian dialogue'¹, where representatives of Athens and Melos negotiate the submission of the Melos Island. During the dialogue, the Athenian envoys asserted *'since you know as well as we do, that right, as the world goes, is only in question between equal powers, while the strong do what they can and the weak suffer what they must.'*

Russia's aggressive 2008 campaign against Georgia and the 2014 annexation of Crimea echo Thucydides' Athenians. Its ongoing deployment of Anti-Access/

Area Denial (A2/AD) capabilities, with offensive and defensive, multi-layered, electromagnetic interference-resistant, cross-networked Integrated Air Defence System (IADS) zones only furthers this message. By preventing enemy combat aircraft from taking advantage of the Freedom of Manoeuvre (FoM), Russia has asserted that it too will do what it can and the weak will suffer what they must.

A2/AD – The Threat

Although there is much debate over the term A2/AD,² it is a useful way to describe the effects of a critical Russian (and Chinese) concept, strategy, and capability. According to the United States (US) Joint Operational Access Concept,³ the following two terms are defined as:



Anti-Access: those actions and capabilities, usually long-range, designed to prevent an opposing force from entering an operational area. Anti-Access actions tend to target forces approaching by Air and Sea, but can also target the Cyberspace,⁴ Space, and other forces that support them.

Area-Denial: those actions and capabilities, usually of shorter range, designed not to keep an opposing force out but to limit its freedom of action within the operational area. Area Denial capabilities target forces in all domains.

Our adversaries generated this A2/AD environment to deter/defend against NATO reactions, inflict an unacceptable political, military, and civilian cost to the Alliance and hence force a negotiated settlement with more favourable terms for their sides. They created these geographically specific zones to support their geopolitical objectives.

Russian and Chinese A2/AD capabilities⁵ span many platforms and multiple domains to generate these effects against the Alliance. Some major categories of capabilities fall under the heading of missiles (cruise and ballistic), IADS, fighter aircraft, submarines, Special Forces, and other non-kinetic assets. A modern A2/AD

concept will simultaneously employ many effects across multiple domains to prevent NATO forces from entering and operating within a specific area. It will use asymmetric methods with non-kinetic assets to deny access to the Space and Cyberspace domains and the Electromagnetic Spectrum to dominate the physical domains. Thus, A2/AD environments are comprised of a system of systems, which overlap and complement each other, mitigating the weaknesses of each and thus making it very difficult to attack any part without another part countering the attack.

When faced with such a system, we discover that it is designed to be difficult to counter. NATO's adversaries have observed the western way of warfare over the past 30 years. They have had time and opportunities to analyse our weaknesses. One factor has been the west's (and NATO's) leverage of superior airpower, giving all our components FoM in all domains. The adversaries did not try to match NATO's battle-winning technology for their air assets and, instead, focused on developing the Surface-Based Air Defence (SBAD) field.⁶ This approach led to advanced IADS and, subsequently, the A2/AD system. A2/AD threatens NATO FoM in all domains; being designed to cause joint problems, it can only be countered with a joint solution. It is also intended to cause 'wicked problems',⁷ in such a way that while solving one aspect of the problem, another becomes critical. This partly happens because, while we talk about a joint fight in NATO, the component-based Joint Task Force is mainly structured to take care of its own component business. Whilst we are set-up to exploit opportunities created by other elements, our cross-component integration is rudimentary. Moreover, employment of Joint Fires is simply not understood enough within the Alliance to exploit its true potential.

A2/AD – Combating the Threat

NATO uses a well-defined F2T2EA⁸ targeting cycle and has some very advanced platforms designed to carry it out. However, traditionally, the Find function has fallen to the wide-bodied Intelligence, Surveillance and Reconnaissance (ISR) air assets, such as the RC 135 Rivet Joint or the E8 JSTARS. Used in combination with

other ISR capabilities, these platforms can detect and track threat systems' movements – which is particularly important considering the mobility of many parts of an A2/AD system. The newer problem is the increased range of these threat systems; they can hold the large ISR assets at risk at ranges of hundreds of kilometres, thus inhibiting their ability and accuracy in performing their F2T2 functions. One solution to this problem came with the advent of low-observable 5th Generation (G5) combat aircraft. They bring step advances in the traditional combat air sphere while also providing sensor suites to rival traditional ISR platforms. However, the unique design of G5 platforms makes the weapon load capacity less than that of the 4th Generation (G4) combat aircraft.

The drawback is that the G5 platforms can position themselves to find, fix, and track advanced targets but do not have the appropriate weapons to engage all targets, if they use their low-observable capabilities.^{9,10} Conversely, the G4 platforms can carry appropriate weapons but cannot get close enough to employ them. Furthermore, G4 platforms cannot use Long-Range Stand-Off Weapons (LRSOW), as the targets in the threat system are highly mobile while the comprehensive planning required for LRSOW employment is not flexible enough.¹¹ Even the GPS-reliant Joint Air-to-Surface Standoff Missile (JASSM), which can be re-programmed in the air, when launched in an attack on coordinates mode can be easily jammed.¹² What is needed is the ability of the G5 platforms to provide the F2T2 service to a flexible and highly reactive weapon system that can be effectively and rapidly employed without itself becoming vulnerable to the threat.

Having examined what makes up an A2/AD environment, we shall focus on the methodology required to defeat it and how it fits within the current doctrine. As we have seen, A2/AD is a joint problem, threatening all domains.

One effective solution is the employment of joint capabilities, enabling a layered approach. Just as the A2/AD is a layered and overlapping set of threats, the way to combat it lies in the use of joint effects that complement each other in degrading the A2/AD whilst negating the threat to themselves. This may mean, for



example, that the sensor and shooter in the kill chain are different actors. This is entirely coherent with the NATO Joint All-Domains Operations (JADO).¹³

The JADO approach¹⁴ presents its own set of challenges; leveraging joint effects requires close cross-component and joint coordination to a higher level than we routinely practice in NATO. However, the increasing complexity of A2/AD and the necessity to use joint effects to counter it means that the development of this doctrine is essential. Various attempts modelled to degrade A2/AD, using conventional Suppression of Enemy Air Defences (SEAD) operations, have consistently shown that the requirement in ordinance when the Air Component attempts it alone is prohibitive. For a realistic chance of success we need to synchronize Joint effects.^{15,16}

An ability to understand how and why to synchronize joint effects is needed. Still, one of the limiting factors is our ability to share information with the correct classification between components and units (sensor to the shooter) at the speed of relevance.¹⁷ This becomes a crucial limiting factor when we must rely, for



example, on a G5 platform finding and fixing a long-range Surface-to-Air Missile site but a Land Component Surface-to-Surface Missile battery is acting as the kill mechanism.

Synchronizing the Joint Effects in Action

So much for the theory. How about the practice? The synchronization of joint effects to counter A2/AD problems has been introduced in recent NATO exercises. The first exercise approached the problem with a 'Tiger Team' mentality. It quickly became apparent that the expertise and understanding needed for this function required a specialized team. This led to the implementation of the Joint Effects Synchronization Team (JEST) in subsequent exercises. The JEST brought together strategic planners, targeteers, and Subject Matter Experts (SMEs) from G5 aircraft, cyberspace, space, and Electronic Warfare (EW) backgrounds, all focused on defeating the A2/AD threat. Formalizing the team also meant that the A2/AD problem could be worked outside of the traditional 72-hour Air Tasking Order cycle, which is critical because many of the required

capabilities have longer lead times to coordinate and benefit from the conditions-based approach of the Strategy Division. This became especially apparent with the inclusion of LRSOW in the counter A2/AD package. While unsuited against all A2/AD threats, LRSOW are capable against certain fixed targets and can be used to expose other A2/AD elements. Employing a 96–120 hour planning horizon allowed more effective synchronization of LRSOW with the traditional strike assets and also enabled similar harmonization of effects from other domains including space, cyberspace, and EW.

Wicked problems, like the A2/AD, can only be tackled through joint, synchronized effects in space and time. Therefore, before the operation (exercise) even started, the JEST developed a broad-brush plan to break the A2/AD into separate elements enabling a comprehensive approach. Ideally, in such a plan each critical target would be addressed with multiple lethal and non-lethal effects, from multiple kinetic and non-kinetic providers from all appropriate domains.¹⁸ Achieving this harmonization requires a JEST populated with members that have a strong understanding of joint capabilities, which enables detailed coordination with

the other components' joint fires SMEs. HQ AIRCOM was fortunate while developing the JEST to have a good working relationship with US Air Forces Europe 603rd Air Operation Center (AOC) Targeting Effects Team and with US European Command's Joint Fires Cell, which enabled rapid process improvement.

While the JEST function is joint by doctrine, and should ideally reside with the Joint Force Commander, the extensive and unusual skills required to plan an A2/AD takedown led AIRCOM to develop an effects integration capability like no other. Thus, with Allied Joint Force Command Brunssum's (JFCBS) agreement, the JEST has continued to reside within the AIRCOM Joint Force Air Component (JFAC) while executing with JFCBS's authority. This clarification of role versus authority was essential to acceptance by the other HQs and was recognized as necessary to address the A2/AD threat. Countering A2/AD threats requires a considerable effort and, if left unaddressed, can lead to other components not receiving the expected level of air support. All components must understand that without tackling the A2/AD threat, the Air Component will not have the FoM needed to provide that air support.

Key Takeaways

The application of this process in the aforementioned exercises allowed for its refinement and improvement while identifying some key takeaways:

- A2/AD systems can only be tackled from a joint approach.
- All components have a vested interest in successfully degrading the A2/AD system.
- The need to increase knowledge across all components of the entire spectrum of joint capabilities and the whole F2T2EA process, and to understand each element's contribution.
- The need to improve the sensor-to-shooter communications process, particularly given that these will frequently occur across components. Compatible and secure communication systems are crucial.
- The Alliance needs more Joint-fires and effects experts. Understanding joint effects at the Component HQ level is lacking; without this expertise, we struggle to achieve the synchronization required to combat the A2/AD threat.

Conclusion

In many ways, the advent of A2/AD threats and the development of methods to counter them are nothing more than the latest iteration of the cavalry being replaced by observation balloons. A2/AD can hinder our ability to 'see over the hill'. We owe it to our front line troops to perfect ways to see what the enemy is doing and influence him. Unlocking the A2/AD problem is key to this and we must continue to perfect the processes we have developed so far, coherent with NATO's JADO concept.

This way, the Alliance can be transformed and prepared for the future challenges of the modern battlespace. Training, education, and future leadership can enhance all aspects of Joint All-Domain warfare,



confirming the consistency of Thucydides' words: *'In practice, we always base our preparations against an enemy on the assumption that his plans are good; indeed, it is right to rest our hopes not on a belief in his blunders,*

*but on the soundness of our provisions. Nor ought we to believe that there is much difference between man and man but to think that the superiority lies with him who is reared in the severest school.'*¹⁹ ●

1. Thucydides, 'The Peloponnesian War', London, J. M. Dent, New York, E. P. Dutton, 1910, <http://www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.01.0200%3Abook%3D5%3Achapter%3D90> (accessed 26 August 2021).
2. The National Interest, Chief of Naval Operations, Adm John Richardson: 'Deconstructing A2/AD', 3 October 2016.
3. Joint Operational Access Concept (JOAC), United States Department of Defence, 2012, p. 6.
4. NATO defines Cyberspace as the global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separate or independent, which process, store or transmit data.
5. A. Schmidt, 'Countering Anti-Access/Area Denial', JAPCC Journal Ed. 23.
6. Franz-Stefan Gady, 'US Air Force: Russia Has Closed Air Power Gap With NATO' in The Diplomat, 16 September 2015, <https://thediplomat.com/2015/09/us-air-force-russia-has-closed-air-power-gap-with-nato/> (accessed 25 August 2021).
7. Horst W. J. Rittel and Melvin M. Webber, 'Dilemmas in a General Theory of Planning', Policy Sciences, Vol. 4, No. 2 (June 1973), pp. 155–169, <https://www.jstor.org/stable/4531523> (accessed 25 August 2021).
8. Find, Fix, Track, Target, Exploit, Assess.
9. John A. Tirpak, 'New longer-range Missiles needed to Preserve Stealth Advantages', Air Force Magazine, 23 September 2021, <https://www.airforcemag.com/new-longer-range-missiles-needed-to-preserve-stealth-advantages/> (accessed 28 September 2021).
10. F35 A/B/C Technical Specifications, <https://www.f35.com/f35/about.html> (accessed 28 September 2021).
11. Mark Gunzinger, 'Stand In, Standoff', Air Force Magazine, 1 July 2020, <https://www.airforcemag.com/article/stand-in-standoff/> (accessed 28 September 2021).
12. Charles Pope, Secretary of the Air Force Public Affairs, 'Roth, Brown, Raymond present Air, Space Forces priorities to Congress', <https://www.af.mil/News/Article-Display/Article/2600678/roth-brown-raymond-present-air-space-forces-priorities-to-congress/> (accessed 27 September 2021).
13. 'NATO JADO, A Comprehensive Approach to Joint All-Domain Operations in a Combined Environment', JAPCC Leaflet, February 2021, <https://www.japcc.org/portfolio/nato-joint-all-domain-operations/> (accessed 27 August 2021).
14. Capt (N) Cochran and Col Willis, 'Transitioning NATO to an All-Domain Mindset', JAPCC Journal Ed. 32.
15. Col Speed and Lt Col Stathopoulos, 'SEAD Operations of the Future: The Necessity of Jointness', JAPCC Journal Ed. 26.
16. Col Speed and Lt Col Stathopoulos, 'Challenges of Future SEAD Operations: An Insight into SEAD in 20 Years', JAPCC Journal Ed. 27.
17. Brig Gen Giuseppe Sgamba, Assistant Director JAPCC, 'The Need for Speed: More and Better Military Tools are Not Enough', JAPCC Journal Ed. 31.
18. Conversation with Lt Col Nuno Monteiro Da Silva, PO AF, and Lt Col Christian Heijnen, NE AF, 1 October 2021.
19. Ibid 1., Book 1, Chapter 4.

Squadron Leader David Tucker

has served in the Royal Air Force (RAF) since 1987. He spent most of his career as a Weapons System Officer on the RAF Tornado GR1 and GR4, and completed an Exchange Tour with the German Air Force flying the Tornado ECR. He completed a MLitt in Strategic Studies at the University of Aberdeen in 2004, winning the Gordon Shephard Memorial prize that year for his essay published in the AirPower Review on European Defence Integration. He has finished a staff appointment at HQ Allied Air Command in Ramstein and currently serves in CAOC Torrejon.



Major Charilaos Nikou

Graduated from the Hellenic Air Force (HAF) Academy with a BSc in Aeronautics in 2003. He holds two MScs in Business Administration from the Technical University of Crete, GR, and International Affairs from Nicosia University of Cyprus. He is a graduate of the Tactical Leadership Programme (TLP). He is an F-16 instructor, a functional check flight pilot, and a command pilot with nearly 2,000 flying hours. He has served in the 343 Fighter Squadron from 2008 to 2020. He is currently serving as the Electronic Warfare, including SEAD Operations, SME at the JAPCC.





Air-Land Integration – Bridging the Gaps in Joint with Force Education and Training

Practical Solutions for Air-Land Interoperability in NATO

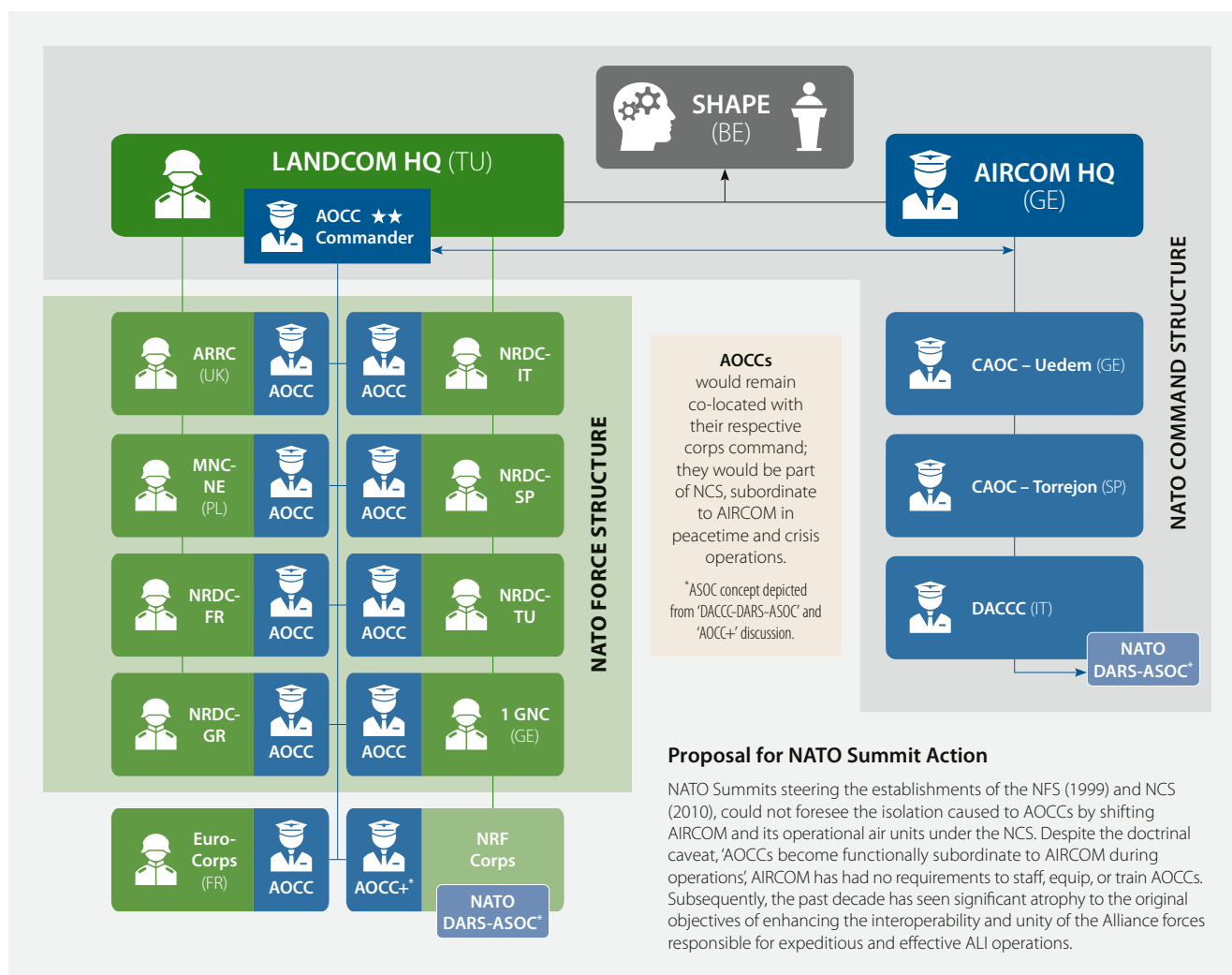
By Lieutenant Colonel Sarah Fortin, US AF, 4th Combat Training Squadron Germany

By Lieutenant Colonel Pasquale Masone, IT A, NATO Rapid Deployable Corps Italy

Introduction

In military and industry circles, it is very common to hear technology promoted as a joint and interoperable capability without much attention being paid to the people employing those capabilities. No matter

how much faith we have in our technological solutions, resilient architectures must always consider, ‘what if a capability is easily denied or disrupted?’ As decisions in warfare are often driven by human endeavours, viable capabilities that enable Air-Land Integration (ALI) and interoperability must be entrusted to



a knowledgeable and united joint force. Simply put, technology alone will not make a joint force interoperable; the people will. Since the article 'ALI – NATO's Strategic Joint Challenge'¹ was published in September 2019, both Allied Air Command (AIRCOM) and Allied Land Command (LANDCOM) have achieved marked progress in addressing the canyon-sized gaps that prevent ALI from being interoperable between their respective components. While initial joint discussions have been productive, there is still extensive work ahead towards achieving all joint ALI objectives, thereby driving the purpose of this article. Given the vast scope of ALI and the interoperability matters, this article will focus on some promising joint collaboration efforts, outline affordable, practical options for immediate joint action to improve ALI, and present an innovative solution to achieve effective joint ALI and interoperability, which could inform reorganization talks of NATO forces in upcoming summits.

A Review of Measured Progress

Following the Joint Analysis and Lessons Learned Centre (JALLC) report on NATO's capacity to conduct ALI, AIRCOM and LANDCOM acknowledged the limitations identified by establishing a joint, two-star led ALI steering group. This signalled the start of a purposeful collaboration between the two components to bridge the fundamental gaps required for ALI to function in NATO.² The first discussions proved productive, resulting in an agreement to have a permanent Land Liaison Element established at AIRCOM HQ. Given the proximity and participation in the joint steering group discussions, the United States (US) Army Europe 19th Battlefield Coordination Detachment offered a small team to begin immediate land liaison functions within AIRCOM HQ. This has permitted an interim bridge for the two components while this agreement formalizes it into the enduring NATO



institutional framework. While establishing permanent liaison positions in each component HQ is a vital step, it is equally important that these two-star level meetings continue to occur regularly to build on the momentum of these early initiatives and to achieve the goals of ALI.

Tactical Options in NATO

While the establishment of an ALI steering group and a Land Liaison Element in AIRCOM are swift and straightforward actions, the JALLC's Joint Analysis Report, titled 'Air-Land Integration: Extending NATO's Tactical Air Command and Control Capability to the Corps Level', has led both HQs to focus efforts on a tactical solution, which is establishing a NATO Air Support Operations Centre (ASOC).³ A common capability to both US and United Kingdom (UK) militaries, the ASOC is employed as the primary control agency for the execution of air operations in direct support of land operations.⁴ Its primary mission is the procedural control of air operations within the assigned airspace, short of the fire support coordination line and up to the Coordinating Altitude.⁵ As an air component asset, the ASOC is subordinate to the Combined Air Operations Centre (CAOC) of the Combined Forces Air Component Commander (CFACC), although, it is located with the supported senior-warfighting land echelon.⁶ Given its proven abilities over the last 20 years of coalition

combat operations for joint fires coordination, responsive re-tasking, and accelerating Close Air Support (CAS) to coalition troops, it is understandable why establishing an ASOC has become a preferred tactical option to enable ALI within NATO. While establishing a NATO ASOC is a reasonable start, it may only exist as a frail and fleeting entity if the durable foundation of standardized joint force education and training is not put forth to support it.

SHAPE's Zero-Sum Game

Taking into account the geopolitical milieu of NATO members reeling from the COVID-19 pandemic and the abrupt exodus from Afghanistan, it is unlikely to gain favour for funding acquisitions of unproven military-specific technology. With this in mind, there is merit to SHAPE's zero-sum requirement for AIRCOM and LANDCOM to pursue the development of an ASOC-like capability organic to NATO. While a zero-sum requirement may seem daunting, there are several existing prospects that could meet SHAPE's directive. More importantly, there are several that could best contribute to laying the durable foundation for joint force education and training, much faster and cheaper than setting up an ASOC. The following sections examine potential and existing ALI capabilities within the NATO Command Structure (NCS) and amongst European-based alliance assets.

A DACCC-DARS-ASOC Option

Since an ASOC is an air component agency designed to enable de-confliction and integration of combat air support to the land component, AIRCOM's Deployable Air Command & Control Centre (DACCC) has been tasked with exploring the possibilities of standing up an ASOC. Given the mobile airspace control capabilities of the DACCC's sub-unit, the Deployable Air Control Centre, Recognized Air Picture Production Centre & Sensor Fusion Post (DARS), it is appropriate that it be considered a prime candidate to either re-role or add the ASOC mission to its capabilities profile. The reasoning is that DARS is mainly staffed with airspace controllers and battlespace managers who could most easily transfer their skills to support the procedural controlling functions essential to an ASOC. As it stands today, adding the ASOC mission, instead of a re-role, would limit the extent to which DARS could support and train with the nine land component corps in the NATO Force Structure (NFS). If this DARS-ASOC option materializes, AIRCOM should coordinate prioritization with LANDCOM to support the designated NATO Response Force (NRF) corps. Ideally, this alignment would bolster standardized joint education and training of the NRF forces to exercise and develop Tactics, Techniques, and Procedures (TTPs). After all, 'the NRF is a driving engine for NATO's military transformation.'⁷

UK's ARRC: An Advocate of ALI Developments

Given that the UK maintains and trains its own ASOC capability, the UK's Allied Rapid Reaction Corps (ARRC) has been LANDCOM's lead to collaborate with AIRCOM on developing options to grow and sustain NATO's own ASOC capability. This joint collaboration has taken on a new significance for the ARRC, since it was identified to lead as NATO's first warfighting corps since the Cold War, effective 1 January 2020.⁸ The ARRC has been trailblazing ALI improvement efforts by working to apply and adapt Joint Air-Ground Integration Centre (JAGIC) US doctrine with the UK ASOC, its Air Operations Coordination Centre (AOCC), and Joint Fires Support Element (JFSE), modelling the potential NATO AOCC+ concept. The JAGIC is a joint seating arrangement that

co-locates air and land operators, Command and Control (C2) systems, and decision-making authorities to facilitate rapid and effective mission execution while managing risk through increased situational awareness.⁹ These efforts and lessons learned should continue to feed into the ALI steering group to identify the requirements to achieve benefits of expediting and synergizing effects by air and land forces.

USAFE-TACP: Bonus Option

Provided that both AIRCOM units and US Air Forces in Europe's Tactical Air Control Party (USAFE-TACP) work for the same commander, it is logical to consider including USAFE-TACP as another enabling contributor to NATO's ALI improvement efforts. It is mutually beneficial for NATO units and USAFE-TACP members to regularly train together and share their ALI expertise with an emerging NATO ASOC capability. Particularly, since USAFE is re-establishing its ASOC capability in Poland, under the 4th Expeditionary Air Support Operations Squadron (4 EASOS). For example, in June 2021, the 4 EASOS participated in Slovenia's premier CAS exercise, Adriatic Strike, paired with a multinational land fires team to showcase the benefits of ALI operations by employing a co-located joint fires C2 team. Furthermore, the TACP instructors from the 4th Combat Training Squadron could be leveraged into promoting joint education and training by conducting mobile training team events to enhance NRF training. Over time, this type of consistent collaboration would grow a knowledgeable network of joint forces that would ultimately strengthen NATO's ALI.

USAFE-AFAPRICA Warfare Centre (UAWC): Reliable Enabler

Understanding that joint education and training is fundamental to the progress of ALI in NATO, the newly designated UAWC, formerly Warrior Preparation Centre, debuted its ASOC-trainer during its premier joint-combined live, virtual, and constructive exercise, Spartan Warrior 21-9. Given the substantial efforts involved with exercise design and execution, UAWC's ASOC-trainer would be another mutually beneficial asset in

streamlining joint-combined education and training for the Alliance. Not only could it serve as an experimental lab for joint experts charged with developing doctrine for NATO's own ASOC capability, it could also serve as a live training node, networked to support exercises, such as, but not limited to, AIRCOM's Ambition and/or NATO's Joint Trident series. Moreover, if network accessibility is made available to connect the ASOC-trainer to AIRCOM, and other relevant NATO organizations, joint training audiences would benefit from experiencing a more holistic picture of the planning and coordination requirements necessary for actual joint operations. The ALI Steering Group should leverage existing joint education and training capabilities of the UAWC to better, and more affordably, prepare its ALI capabilities for large-scale combat operations and improve the interoperability of the allied joint forces.


Unifying ALI for NATO Joint Forces

A shift in perspective to address joint solutions by means of people is in order, and it can have maximum benefits coming as a result of a NATO Summit decision. While there have been some voluntary collaborations amongst units in the NCS and NFS, the current command relations' hierarchy does not mandate, nor facilitate, a normalized solution that fosters joint personnel interactions between the two structures. More specifically, what was intended to bring joint forces together is actually perpetuating the divide. The creation of the

NCS, an outcome of the 2010 Lisbon Summit, has inadvertently stifled any obligation for AIRCOM to staff, equip, and train the AOCCs, a standing, yet isolated, air component liaison element, attached to each NATO Corps under the NFS. Consequently, the interests and obligations for staffing, equipping, and training between the AOCCs vary significantly. Therefore, the shift in perspective must seriously consider realigning the responsibility of AOCCs under AIRCOM, otherwise there is risk of the complete regression of NATO ALI interoperability. The last decade of ALI, under the current hierarchy, has stumbled along under the triaged doctrinal pretence that AOCCs become functionally subordinate to the NCS Joint Force Air Component during operations.¹⁰ However, the question of how this would actually occur has only recently come to light. A realignment of AOCCs under AIRCOM is not too far-fetched when considering the 'NATO 2030' vision, discussed at the 2021 NATO Brussels Summit.¹¹ A realignment would be a way to produce tangible results that cultivate genuine joint force interoperability and support several strategic lines of efforts outlined in the initiative. While this shift would likely not be entirely zero-sum, it would offer a course correction to the intended relationship between NCS and NFS that would pay dividends to benefit future NATO forces and joint operations. To this end, joint interoperability requires that all HQs that may command operations in theatre are staffed, trained, and prepared to a common standard.¹²

Conclusion

Bridging the gap in joint with force education and training is essential. More specifically to the realm of ALI in NATO, a focus on providing a standardized education



4th Combat Training Squadron JTAC Instructor providing instruction during Close Air Support training at Baumholder military training area in Germany. JTACs are essential to the tactical and operational ground elements in coordinating and facilitating effective Air-Land Integration for NATO.

and training programme for the corps' AOCCs, JFSEs and joint liaisons will establish a robust foundation. Standing alone, an ASOC will not produce effective ALI unless the core of joint forces, who will affect it, understand its design, doctrine, and TTPs through joint education programmes before it is practiced in joint training. Investigation into the education of joint ALI elements will carry great value, in dynamic operations, stemming from a common understanding of each component's capabilities, procedures, and limitations. In view of the most practical DACCC-DARS-ASOC option, the combination of such an element with a dedicated joint educational programme, like the ALI Workshop, would propel a durable joint learning programme while keeping close to SHAPE's zero-sum requirement.¹³ Such an ALI enterprise, backed by the ALI Steering Group and a NATO Summit agreement for AOCC realignment, would set the course for improving the Alliance's joint readiness, responsiveness, and ability to maximize collective defences, especially during resource constraining conditions. In the end, these

actions would contribute to the efforts outlined in the 'NATO 2030' vision, that unified forces enhance NATO's collective ability to deter, defend, and win against any attack, in any domain. ●

1. S. Fortin and L. Rossetti, Air-Land Integration – NATO's Strategic Joint Challenge, *The Journal of the JAPCC*, Ed. 30 (2020), p. 46–52.
2. JALLC/CG/20/034, Air-Land Integration: Extending NATO's Tactical Air Command and Control Capability to the Corps Level, March 2020.
3. Ibid.
4. Joint Publication AJP 3-30, Joint Air Operations, NATO Standardization Office, July 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf (accessed 20 May 2021).
5. Ibid.
6. Ibid. 4.
7. NATO Response Force, March 2020, https://www.nato.int/cps/en/natolive/topics_49755.htm (accessed 21 April 2021).
8. Corps Strength – Allied Rapid Reaction Corps Prepares For 'Demanding' New Role, November 2019, <https://arrc.nato.int/newsroom/archive/2019/20191129> (accessed 5 June 2021).
9. UK Joint Air Ground Integration Centre Handbook (v 6.1), January 2019.
10. Allied Joint Publication AJP-3.3, Allied Joint Doctrine for Air and Space Operations, Ed. B, Ver. 1. NATO Standardization Office, 2016.
11. On the Agenda, June 2021, https://www.nato.int/cps/en/natohq/news_184633.htm#9 (accessed 20 July 2021).
12. Ibid.
13. Ibid. 1.

Lieutenant Colonel Sarah V. Fortin

earned her commission as a distinguished graduate of the Reserve Officer Training Corps in 2004. She is a Senior pilot with more than 1,950 hours, including combat time over Iraq and Syria, in the C-130E/H Hercules and B-52H Stratofortress. During previous assignments, she served as an Air Liaison Officer to V Corps and HQ US Army Europe in Germany. While assigned to the DACCC from 2017 to 2020, she served as the Chief of Dynamic Targeting and Time-Sensitive Targets Cell, as Chief of the Air-Surface Integration Team and as a NATO-qualified nuclear planner. Currently, Lieutenant Colonel Fortin is the Director of Operations for the 4th Combat Training Squadron, USAFE-AFAFRICA Warfare Center, Einsiedlerhof Air Station, Germany.



Lieutenant Colonel Pasquale Masone

was commissioned in the Italian Army in 1995 as an artillery officer and served as Section Commander, Battery deputy commander and forward observer until 2001 when he qualified as a CBRN officer and was posted in the Italian Army CBRN Defense Regiment where he served until 2007 as G3 CBRN. In 2008 was posted to the 1 Army Aviation Support Regiment where he was a Squadron Commander until 2010. The same year he was assigned to the HQ ARRC in UK as battlespace manager and in 2011 he deployed to Afghanistan where he served as the ISAF IJC Battlespace manager. Back in Italy in 2013 he was commissioned to the Italian Army Targeting and Info Ops Center as a targeting and joint fires officer/instructor.





Defending Space in and through Cyberspace

A Fragile Stability in Space

By Major Fotios Kanellos, GR AF, JAPCC

Introduction

In a recently published book titled '2034',¹ Admiral Stavridis and Elliot Ackerman, two former military officers with deep operational and diplomatic backgrounds, tried to describe how and, apparently, when a future war with China might start. The novel provides a frightening view of an Orwellian dystopian future where the two global powers, the United States (US) and China clash, whereby powerful new forms of cyberspace weaponry and stealth capabilities are employed. According to the scenario, the hypothetical future war starts when the Chinese block the

communications systems between the ships in the Pacific Ocean, thus blinding not just the entire fleet but also the US National Command Authority.

Although the book refers to a far-in-the-future nightmarish US-Chinese military conflict, one might claim that all the mentioned trends and disruptive technologies, no matter how fictional they seem, are real, present, and ready to be used in today's modern military arsenals. Effective communications and navigations services, provided by space-based systems, are extremely vital for advanced militaries, global economies, and societies. Climate and natural disaster monitoring,

early warning systems, weather forecasting, global imaging, commercial communications systems, precise positioning, navigation, and timing synchronization, as well as surveillance and reconnaissance, are just a few of the core space-based technologies which our daily lives are totally dependent on.²

A Newly Born Domain

Since the beginning of the 21st century, technological advancements have led to increasingly affordable space capabilities for various stakeholders, including governmental, academic, and commercial entities. Launching satellites into orbit is not the sophisticated and insanely expensive activity that used to be practiced only by a handful of state superpowers. Today, small businesses, private individuals and even academic institutions can afford to manufacture, launch, and operate satellites. This leads to the ever-expanding commercialization of space activities contrary to the military domination of the domain in years past.³ Notably, with the advent of 5G and 6G mobile networks, satellites are expected to play a far more central role to provide the nearly ubiquitous, instantaneous, and maximum connectivity those networks are promising.⁴

As recently as the 15th of September 2021,⁵ the private spaceflight company SpaceX launched four civilian passengers into orbit on the first-ever mission to space with an all-civilian crew. A few months earlier, two other private spaceflight companies, Virgin Galactic and Blue Origin, launched capsules into sub-orbital space, highlighting the evolution of human spaceflight and the ease of access to an area, which was previously dominated only by governments and their space agencies.⁶

Simultaneously, the rapidly increasing number of small satellites, nanosatellites, and microsatellites in outer space has exponentially multiplied the sheer volume, diversity, and global coverage of the produced data. To collect, process, and analyse this data, newer applications and services enabled by revolutionary technologies such as artificial intelligence, quantum computing, and automation had to be created. This new era

for space, known as the 'New Space Phenomenon',⁷ has created new business opportunities and opened new markets around the world,⁸ thus increasing the growth and dependency of civil and military actors on space systems and services.

In the face of these developments, on the 4th of December 2019, the NATO Alliance adopted NATO's Space Policy and recognized space as a new operational domain alongside air, land, sea, and cyberspace.⁹ Based on the use of satellites, NATO can now respond to crises faster, more effectively, and precisely. The recognition of Space as an Operational Domain emphasizes exactly its dynamic and rapidly evolving inherent capability to enhance the Alliance's deterrence and defence posture in an age of global competition.¹⁰

Space Threat Categories

Modern space services and capabilities such as the Global Navigation Satellite System and Satellite Communications, used by both the military and civilian sectors, are considered critical national infrastructures.¹¹ These core space-based technologies have become vital assets for public safety, economic welfare, and national security of all advanced countries. However, the threats and vulnerabilities of commercial satellites and other space assets have also increased significantly during recent years, especially due to the dynamically evolving cybersecurity threat landscape.

Of course, the weaponization of space is not only facilitated through the cyberspace domain. A US report, published in 2018, argues that China and Russia are developing space weapons¹² ranging from non-kinetic physical attacks to ground sites and infrastructure to kinetic direct ascent attacks against orbiting assets. Additionally, on the 27th of March 2019, India had successfully tested its first Anti-Satellite (ASAT) missile (mission Shakti),¹³ becoming only the fourth nation to possess such a capability. In recognition of the growing threat in the space domain, on 8 March 2021, France launched its first-ever military space exercise 'Aster X 2021' simulating various space events and scenarios.¹⁴

Among the many emerging threats to space systems, the most apparent, irreversible, and likely attributable are the kinetic physical threats. These threats include attacks on static Command and Control (C2) facilities, detonations of warheads near the orbital path of a targeted satellite, and direct ascent ballistic missiles against specific satellites. More advanced versions of a co-orbital attack may also include robotic arms able to grab another satellite, thus displacing or destroying it.¹⁵ After all, satellites are lightweight devices moving at incredible speeds on predictable paths and, therefore, are extremely fragile; even a miniscule projectile can destroy them.

The threat category, which may be considered the biggest and most likely threat to the space assets, is the non-kinetic one. Without any direct physical contact, these threats can attack satellites and ground stations at the speed of light, without being observed by third parties and, thus, are difficult to attribute to one particular nation. These threats include directed energy weapons capable of damaging sensitive components and blinding critical satellite sensors, electronic attacks

(jamming or spoofing) against radio frequency signals of the up- and down-links, and sophisticated cyberattacks targeting network components, processing units, and data streams.

Cyber Threats to Space Assets

As space has developed in modern times to become the 'ultimate high ground' of information-age warfare, so too has the space arms race intensified and focused on more interconnected and computational complex cyberattacks.¹⁶ During the 20th century, the so-called 'old space' or 'traditional space' systems were designed for long-lasting missions and tailor-made solutions.¹⁷ These systems were not built with sufficient security mechanisms that would protect them from the unique and constantly evolving characteristics and challenges of cyberspace threats.

The cyberspace domain consists of a fluid, highly contested, congested, cluttered, connected, and constrained environment. As a result, the cyber threat landscape is evolving with tremendous speed, bringing new vulnerabilities and challenges to the surface. Billions of connected Internet of Things (IoT) devices have enlarged the attack surface with a diversity of attack vectors.¹⁸ Moreover, cyberattacks can be almost instantaneous, global, asymmetric, invisible, and catastrophic without even reaching the threshold of an armed attack.

Different types of threat actors are persistently trying to exploit any possible weakness in and through cyberspace to maximize the destructive effects in the space domain. Nation-states, state-proxies, cyber terrorists, criminals, hacktivists and even insiders are considered potential actors to develop sophisticated offensive cyber capabilities targeting the vulnerabilities of space systems. The potential high impact supplemented by

the low costs and minimum resources needed entices threat actors towards cyberattacks as a primary means. Whilst many of the tactics, techniques, and procedures developed in the cyberspace domain can be extensively adapted, reused, and shared among adversaries, avoiding the need for new toolsets and skills.

Cybersecurity requirements have to be applied to all segments that comprise an operational space system. These segments include the space, ground, link, and user portions. Significantly, the last three components rely on data systems and networks that can be compromised by injecting malicious code. Some of the most common types of cyberattacks, the distributed denial-of-service, man-in-the-middle, ransomware attacks, botnets, Advanced Persistent Threats (APTs) and the use of privacy-enhancing technologies, have developed so much that the conventional network defence tools, such as intrusion detection and prevention systems, and antiviruses may seem obsolete.¹⁹

Cyber Kill Chain

Well-resourced and trained adversaries targeting highly sensitive and national security information tend to conduct multi-year intrusion campaigns using advanced tools and techniques described as APTs. An APT method can stay undetected in a system or network until it fulfils its predetermined goals.²⁰ Those APT actors, following a kill chain model, attempt long-term and multiple intrusions and adjust their strategy based on the results – positive or negative – of these attempts.

A kill chain 'is a systematic process to target and engage an adversary to create desired effects.'²¹ According to the US military targeting doctrine, this process consists of the following steps: Find, Fix, Track, Target, Engage, and Assess. This integrated, end-to-end process is similar to a 'chain' in which all links must be fulfilled to complete the task.

Similarly, the cyber kill chain model describes the phases from conceptualization through to achieving the desired effects with respect to computer network attacks or espionage and was first introduced by Lockheed Martin.²² These phases include Reconnaissance, Weaponization, Delivery, Exploitation, Installation, C2 and Actions on Objectives. Following these steps, the aggressor tries to develop a payload to breach a trusted boundary, gain authorization inside the trusted environment, and take actions towards his original objectives. These objectives may



be data exfiltration, disrupting the confidentiality of the victim's environment, or violations of data integrity and availability.

A Cyber-ASAT Case Study

One of the most critical areas of spaceflight operations is the collection and use of Space Situational Awareness (SSA) data. Almost all space stakeholders, including the US, Russia, China, and the European Space Agency, have developed modern SSA platforms. These platforms are responsible for delivering timely and accurate information from the space environment to protect both orbit and ground infrastructure.²³ Today, millions of objects of various sizes are travelling in Earth's orbit, at velocities in excess of 8 km/s that can cause catastrophic failures to satellites and launchers. Reliable tracking and prediction of potential collisions with those objects are essential for the spaceflight controllers to navigate the satellites accordingly.

However, a study from 2019 tested the development of a simulated cyber-ASAT capability that could leverage orbital simulations and genetic algorithms to artificially alter debris collision forecasts and cause direct

harm to critical space systems without firing a single rocket.²⁴ This research proved that a sophisticated cyberattack, based on the intrusion kill chains described above, can gain access to SSA's database and manipulate the objects' coordinates. A continuous, updated and transnational SSA data repository needs an extensive network of sensors distributed around the planet, providing an extensive and dynamic attack surface with numerous entry points to exploit.

An attacker taking advantage of backdoors in the network perimeter can alter the datasets so that a near-miss between the targeted satellite and a debris object can be misinterpreted as a collision. As a result, the controller will try to execute unnecessary corrective manoeuvres consuming valuable resources of the satellite and, thus, shortening its lifetime. Vice versa, the attacker may conceal a projected collision with debris depriving the controller of the ability to respond in a timely manner and save the satellite.

Conclusion

Since space systems, both military and commercial, have been considered essential parts of the NATO Nations' critical infrastructure, it is vital to address all cyber

concerns and challenges effectively for their protection. Specific cybersecurity principles and practices must be applied in every phase of the space component's development life cycle process. As the lifespan of satellites may exceed 15 years, it is critical to integrate, already from the design stage, sophisticated cybersecurity – and cryptographic – solutions, which allow the controllers to remotely install updates and to be able to respond to incidents when necessary.

The development and implementation of comprehensive cybersecurity plans for all system elements will provide the requirement for high-level cybersecurity hygiene across a whole range, from detecting network intrusions to managing the supply chain risks of all manufactured products. Therefore, the Alliance must protect their space assets and ensure continuity of operations by strengthening the national and collective resilience of their respective critical infrastructure. ●

1. F. Fukuyama, '2034', 7 July 2021, <https://www.americanpurpose.com/blog/fukuyama/2034/>, (accessed 8 October 2021).
2. J. Fritz, 'Satellite Hacking: A guide for the Perplexed', Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies, Vol. 10, No. 1, December 2012–May 2013, pp. 21–50, 2013.
3. T. Lohela, 'Addressing hybrid threats in the interconnected air and space domains', Hybrid CoE Record 27, February 2021.
4. M. Griffith and C. Hocking, 'Seizing Opportunities: Four National Security Questions to Ask about the Use of Satellites in 5G Networks', September 2021, <https://www.wilsoncenter.org/publication/seizing-opportunities-four-national-security-questions-ask-about-use-satellites-5g>, (accessed 8 October 2021).
5. D. Chow, 'SpaceX makes history with first all-civilian spaceflight', 16 September 2021, <https://www.nbcnews.com/science/space/spacex-makes-history-first-civilian-spaceflight-rcna2027>, (accessed 8 October 2021).
6. D. Chow, 'Virgin Galactic's rocket reaches edge of space with Richard Branson on board', 11 July 2021, <https://www.nbcnews.com/science/space/branson-virgin-galactic-space-launch-n1273547>, (accessed 8 October 2021).
7. Ibid. 3.
8. T. Harrison et al., 'Defense against the Dark Arts in Space', Center for Strategic & International Studies, February 2021, <https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons>, (accessed 8 October 2021).
9. Ibid. 3.
10. NATO, 'NATO's approach to space', https://www.nato.int/cps/en/natohq/topics_175419.htm, (accessed 8 October 2021).
11. Space Policy Directive – 5 (SPD-5), September 2020, <https://fas.org/irp/offdocs/nspm/spd-5-fs.pdf>.
12. G. Baram and O. Wechsler, 'Cyber Threats to Space Systems', June 2020, JAPCC Read Ahead 2020, <https://www.japcc.org/cyber-threats-to-space-systems/>, (accessed 8 October 2021).
13. Drishti IAS News, 'Mission Shakti, ASAT and India', May 2019, <https://www.drishtiias.com/daily-updates/daily-news-editorials/mission-shakti-asat-and-india>, (accessed 8 October 2021).
14. M. Delaporte, 'ASTER X 2021: Putting French Military Space Strategy in the New Space Orbit', April 2021, available at <https://operationnels.com/2021/04/10/aster-x-2021-putting-french-military-space-strategy-in-the-new-space-orbit/>, (accessed 8 October 2021).
15. Y. Tadjdeh, 'U.S. Strengthening Space Domain Awareness', National Defense Magazine, July 2021, <https://www.nationaldefensemagazine.org/articles/2021/7/30/us-strengthening-space-domain-awareness>, (accessed 8 October 2021).
16. J. Pavur and I. Martinovic, 'The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space', 11th International Conference on Cyber Conflict, CCD COE, May 2019, https://www.researchgate.net/publication/334422193_The_Cyber-ASAT_On_the_Impact_of_Cyber_Weapons_in_Outer_Space, (accessed 8 October 2021).
17. H. Grest, 'New Space', JAPCC Journal 29, <https://www.japcc.org/new-space-advantage-or-threat-for-the-military/>, (accessed 8 October 2021).
18. L. Maglaras and I. Kantzavelou, 'Cybersecurity Issues in Emerging Technologies', October 2021, CRC Press.
19. A. Nisioti et al., 'From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods', IEEE, July 2018, <https://ieeexplore.ieee.org/document/8410366>, (accessed 8 October 2021).
20. E. Hutchins et al., 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains', Lockheed Martin, January 2011, <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>, (accessed 8 October 2021).
21. Ibid.
22. P. MacKenzie and F. Kanellos, 'A Comprehensive Approach to Countering Unmanned Aircraft Systems: Cyberspace Operations', JAPCC Book 2020, <https://www.japcc.org/c-uas-cyberspace-operations/>, (accessed 8 October 2021).
23. Ibid. 16.
24. Ibid.

Major Fotios Kanellos

graduated from the Hellenic Air Force (HAF) Academy in 2003 as an Electrical Engineer specializing in Telecommunications and Computer Science. He holds three Master degrees, one in Technical-Economic Systems from the National Technical University of Athens (NTUA), one in Environmental Sciences from the University of Patras and another in European and International Studies from the National and Kapodistrian University of Athens.

He served as an inspection engineer for T-2 C/E aircraft and system engineer for the T-6A Flight Simulator at the Hellenic Air Training Command in Kalamata. His previous appointment was at the HAF Support Command managing IT and Cybersecurity projects. Currently, he is the Cyberspace SME at the JAPCC.



Possibilities and Limits of a C2 (R)Evolution

By Lieutenant Colonel Andreas Schmidt, GE AF, JAPCC

Introduction

Military planners often focus on the development of individual capabilities without considering how they will work in concert with the rest of a nation's forces or let alone allied forces. As with any fine symphony orchestra, harmonizing these capabilities requires a

world-class conductor. Command and Control (C2) systems – and their operators – are the military equivalent of the conductor. It is intuitive that an improved C2 system can increase military efficiency and effectiveness, comparable to the orchestra playing more swiftly and striving for the perfect performance. However, what is actually considered a C2 improvement



and how will such *improvements* be judged? Is it simply that a new C2 system can be considered better if the cost/benefit ratio at the strategic level is *improved* while controlling the same effect-delivering tools, or does *improvement* involve more aspects? The main factors for such improvements could be an increase of overall speed and a decrease in friendly force attrition. Assuming that the outcome of a fair one-on-one duel between two competing systems at the tactical level is a relatively statistical coin toss, this *fair* balance needs to be influenced by the advantages gained from the tactical to the strategic levels. The following will look at some options and their benefits, as well as their drawbacks.

Situational Awareness

One way to skew the balance and improve the effect-delivery of individual systems is to achieve better Situational Awareness (SA) than the opposing systems, which should enable optimized and faster decisions. This requires that all necessary information is available in time for each process (e.g. planning, deployment, engagement) to create an advantage. This is often also called *information superiority*.¹ The sheer amount of active and passive sensors (including both technical and human) available to NATO and its nations, from all domains, produce massive volumes of data. The next steps are converting data to information and then possibly to knowledge,² followed by its dissemination to the required users. Hypothetically,

assuming that the continuous data and information sharing of national sources is given, it needs to be decided what can, will, and must be delivered, and to whom. The knowledge to information conversion before transmission requires trust, but also needs to utilize less bandwidth to save time when serving more than one user. Trust applied to digital content is sometimes referred to as *e-trust*.³ However, this reduces the options for context analysis by a local commander/operator, which, in turn, emphasizes the need for data/information veracity. Additionally, the more data/information that is available, the more imperative 'what is relevant' must be determined to create the advantage. Practically, this can only be done closer to the point of collection, unless the client knows exactly what he actually needs. This becomes less likely with the growing amount of available material, amplified by the bottleneck of distribution through existing networks. In addition, with the increasing volume of data, the actual need for computerized analytical support increases, which is true for detection, classification, identification, and the categorization of relevant data. This is where the constantly evolving fields of Artificial Intelligence (AI),⁴ Big Data,⁵ Deep Learning,⁶ and Quantum Computing⁷ can help to increase speed and efficiency.



Such enhanced efficiency also has its drawbacks. Not only do we have to think about, and deal with, new types of misinformation, since it has a different meaning for an AI than for the human operator,⁸ but also the potential final recipients of the misinformation need to be trained accordingly. The human decision-making process is based on two types of reasoning: 1) more time-consuming deliberative reasoning, and 2) automatic reasoning for routine decisions. Studies have shown that humans tend to use more automatic reasoning when interacting with automated systems.⁹ The faster the system, the less likely the operator will use deliberative reasoning. The debate about *killer*

*robots*¹⁰ revolves around automated or autonomous decisions, lacking the meaningful human control when using lethal force. This can be avoided by keeping these decisions in human hands. However, if the operator is not well trained, there could be little difference in the outcomes in some instances.

To use Surface-Based Air and Missile Defence (SBAMD) systems as an example, external cueing data allows for optimized emissions control and, therefore, later radiation detection and fewer electronic counter-measures. This also supports the optimization of intercept points and the employment of advanced fire



control concepts¹¹ like engage- or launch-on-remote. However, following several fratricide incidents by SBAMD units in Operation Iraqi Freedom, a United States Department of Defense report¹² stated three shortfalls, which led to these sometimes-fatal circumstances. Firstly, critical identification systems performed poorly; secondly, there was a significant lack of SA in the air defence systems; thirdly, the SBAMD concept of operations did not match the actual operational conditions, yet the operators were trained to trust the system. This supports the notion that technical options need to go hand in hand with operational requirements and, most importantly, adequate training.



System of Systems in a Multi-Domain Environment

The overall efficacy of a military action relies on the capabilities used and the way they are employed. Enhancing either will surely improve the outcome. However, just optimizing existing capabilities and processes will have limits, e.g. technical limitations or procedural insufficiencies, to achieve the necessary effect. This might necessitate the development of completely new approaches or capabilities. In the end, the result needs to deliver the envisioned benefits whilst remaining robust for contingency circumstances.

One-on-one or one-on-many engagements are the individual puzzle pieces of every military confrontation, however, the overall purpose is to achieve a desired strategic end-state when using military force.¹³ Aside from individual system effectiveness, the art of military operations is to employ the selected military forces in concert to create overall advantage. At the operational/tactical level, the goal is to employ individual systems as synergistically as possible. Over the recent decades, the significantly increased SA has allowed military operations to switch from a more attrition-focused approach to a more effects-based idea. Furthermore, the ability to network military forces allows for increasingly dynamic joint and combined operations. In current NATO operations, a Joint Force Component leads the individual domain components (e.g. Joint Force Air Component), which provide capabilities in their respective domains. This necessitates, for example, the robust joint coordination of combined forces for target and protected assets prioritization, while still employing a domain-centric focus on effect-delivery itself. In this regard, a SBAMD unit, led by the air component, can provide coverage of an asset requested by the land component, or receive land or naval support for offence-defence integration. Despite joint coordination, domain planning remains mostly at the domain component level. One method to gain an advantage is to plan and execute faster than the opponent's planning cycle, denying the adversary an opportunity for optimal execution. The better the overall SA, the better the military planner can define and understand the *problem space*.¹⁴ All of our available

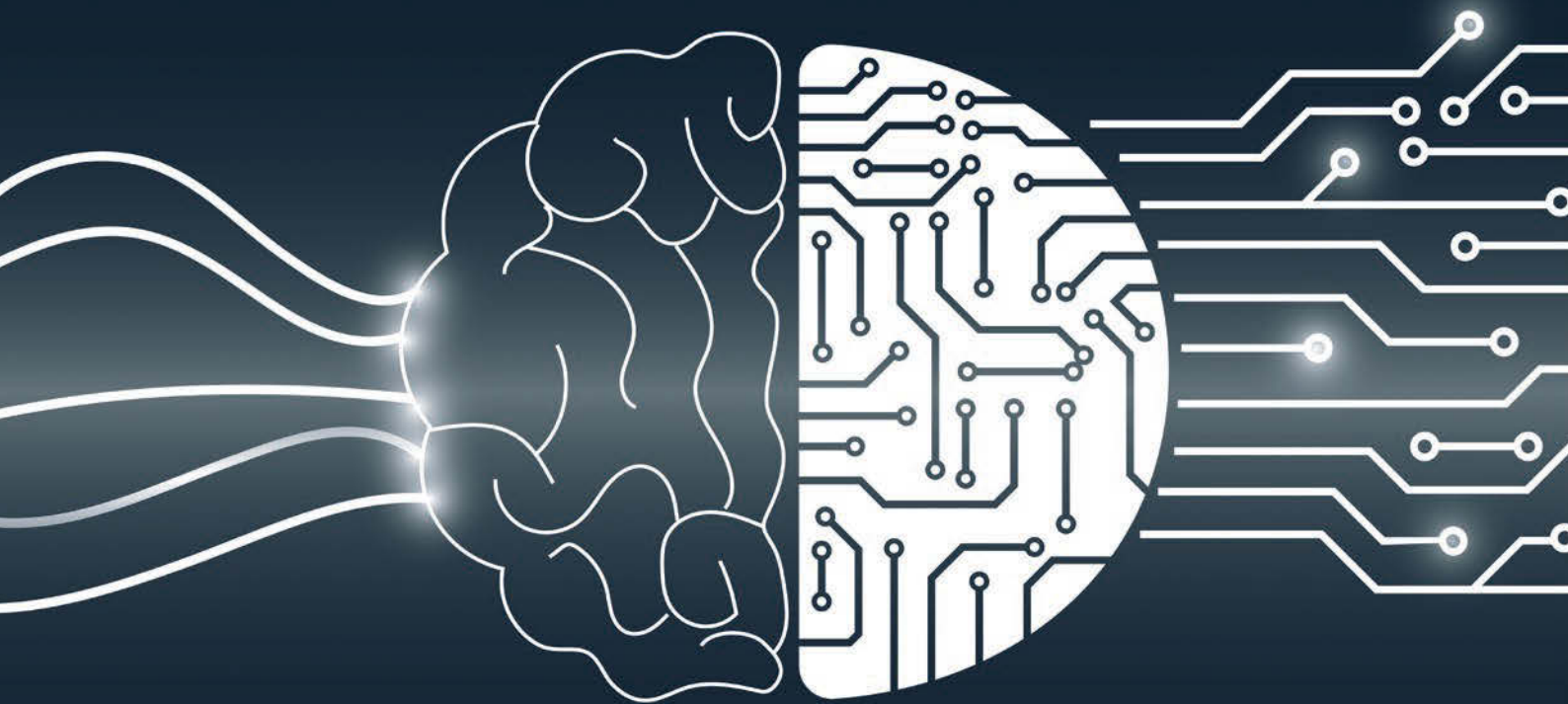
effects, which will help transform the *problem space* into our desired end-state, can be considered the *solution space*.

When thinking in terms of effects, the anticipated odds of applying an effect successfully needs to be maximized. There are two ways of achieving this: by using new weapons, like hypersonic glide vehicles, which promise a high probability of success by exploiting adversary capability gaps, or by combining various capabilities from one or more domains to degrade an effective countermeasure. Every delivered effect changes our *problem space*, which has a subsequent effect on our plans. Currently, air operations and associated air tasking orders are typically planned and executed in 72-hour cycles, allowing for adaptation to *problem space* changes.¹⁵ Other component commands have different planning cycles, which are synchronized at the joint level. With optimal *problem and solution space* awareness at the joint level, supported by available networks and modern software tools, this process can be streamlined to reduce the length of planning cycles and to include solutions with a more robust use of effects from multiple domains towards one objective with less extensive coordination. In addition, the relationship between supporting and supported units should become more flexible in multi-effect missions, since the chosen command relationship construct could be ad-hoc, effect-dependent, and less long-term mission centric. This even more centralized planning and decentralized execution will further transform domain components into mostly capability custodians and effect providers. The military *decision space* will move up in the C2 hierarchy, with the lowest level military entity planned to be the provider or contributor of a *robust* effect, while *robust* has to be defined from a multi-domain viewpoint. This might also have an impact on which and how nations contribute forces to NATO operations, since the ad-hoc, agile force planning can be stymied by the national *red-card holder* concept.¹⁶ For execution, at the tactical level, the magnitude of the change is dependent on the versatility of the tactical capability in affecting the battlespace and providing broader effects. Highly mobile air assets, especially those with a wide spectrum of payloads for various effects, could be used even more flexibly and effectively than before. SBAMD systems, in general, will

benefit greatly from improved SA, resulting in optimized firing and emissions control doctrines, better shot management of layered defences and an overall better use of the defensive inventory. However, the level of unit mobility will have a significant impact on the added value for flexible employment decisions. Long-range SBAMD units have relatively low mobility, which won't allow for very rapid, long-distance re-deployments to cover ad-hoc mission changes. Short-range SBAMD units, however, have higher mobility and will be able to provide coverage in a more flexible way. With significantly increased SA and enhanced planning and execution tools (e.g. AI-enabled) at the joint level, it could be possible to bring a construct like Joint All-Domain Operations¹⁷ to life. This could, in turn, enable faster planning-to-execution cycles, multi-domain dilemmas for the opponent and concentration of an effects-based approach towards the desired end-state. Although it sounds promising, this approach has at least two downsides that must be considered.

Downsides of C2 Relying on Technological Constructs

The development of new C2 constructs based on new technological achievements is not an original idea. We can assume that our potential adversaries are working on similar concepts, also that they are speeding up the operational tempo. Keeping sufficient SA for an adequate understanding of the *problem space* will become more complex. Additionally, our decision cycle must constantly speed up to be able to inject effects into the opponent's planning process. Since the use of human operators itself represents a limiting factor when it comes to processing speed, new C2 constructs have to rely more and more on technological solutions. This might lead to the military equivalent of a *technological singularity*,¹⁸ a *battlefield singularity*,¹⁹ where human cognition can no longer keep up with machine speed. Therefore, by starting the process of speeding up future warfare with the help of computers, AI, or deep learning, we must be aware of the consequences to the overall process. In addition, our ethical and judicial framework must address this dilemma as well. For a moment, let us consider that this challenge can be met and a viable C2 construct of



future warfare created. The human actor/operator, from the political/strategic level down to the tactical level, needs to adapt and train to function in such an environment. Thinking in fast-paced, multi-domain effects terms requires specialized and empowered personnel. Since, from an engineering perspective, it is easier to develop something against an existing capability, it can be assumed that future adversaries will design options to interrupt or negate this new environment. For example, an adversary could use quantum computing to decipher our secure communications, which would significantly impact availability, reliability, and secrecy of data/information. Therefore, a contingency plan needs to be prepared, available, and exercised. This contingency plan requires not only the availability of fall-back technology for planning, execution, and communication, but also the human capacity to remain proficient in both future and *current* C2 constructs. With limited military equipment and available time, this could become a challenge for resource management. A current example is our reliance on Position, Navigation and Timing (PNT) systems such as Global Positioning System (GPS). GPS makes warfare significantly more efficient and effective, but denial of this service is relatively easy using simple tactics such as jamming or spoofing of GPS signals.²⁰ Therefore, soldiers need to be able to use the benefits of PNT, recognize the potential for interference, but also retain the ability to execute their missions without GPS. A good example of GPS interruption in the SBAMD realm is the accurate emplacement of sensors and shooters for

correct engagements and the provision of an unambiguous air picture without PNT service. Therefore, both methods, with and without GPS, constantly have to be practiced. However, the increasing reliance on technological solutions in future complex C2 systems bares similar issues. The overall system needs to be prepared to function under all circumstances. The more robust the underlying technology for future C2 constructs becomes, all-encompassing from core (e.g. Intelligence, Surveillance and Reconnaissance platforms or planning/execution tools) to enabling systems (e.g. communication networks or PNT), the less we have to think about legacies; but this will be costly and time-consuming. Robustness of a system, defined as operating correctly in the presence of exceptional inputs or stressful conditions,²¹ can only be tested against all currently imaginable conditions and inputs. Therefore, robustness needs to be continually reassessed and constantly maintained, especially in a rapidly evolving environment.

Conclusion

Technical innovations have always allowed for improvements in military warfare. Still, just because something is technologically feasible, that does not mean it can be incorporated with ease or without side effects. Optimized SA and more capable tools will always allow for better and faster planning and execution. However, this capability needs to be as robust

as possible in all anticipated scenarios, backed by suitable fall-back options. All personnel must be sufficiently educated and trained in both worlds and able to switch seamlessly between the two. Also, the increased speed of military operations, due to technical support, must be balanced with human capabilities in an ethical and legal framework. The more complex systems become, the more emphasis needs to be placed on maintaining robustness and resilience in a constantly evolving environment. It is not about a one-time procurement of a C2 toolkit, rather the constant evolution of systems and the requisite education and training of the operators at all levels. Giving the orchestra some new instruments or a new conductor will certainly require fine-tuning, continuous rehearsal, and a genuine performance review, always with a fall-back option to replicate familiar quality standards to satisfy listener's expectations.

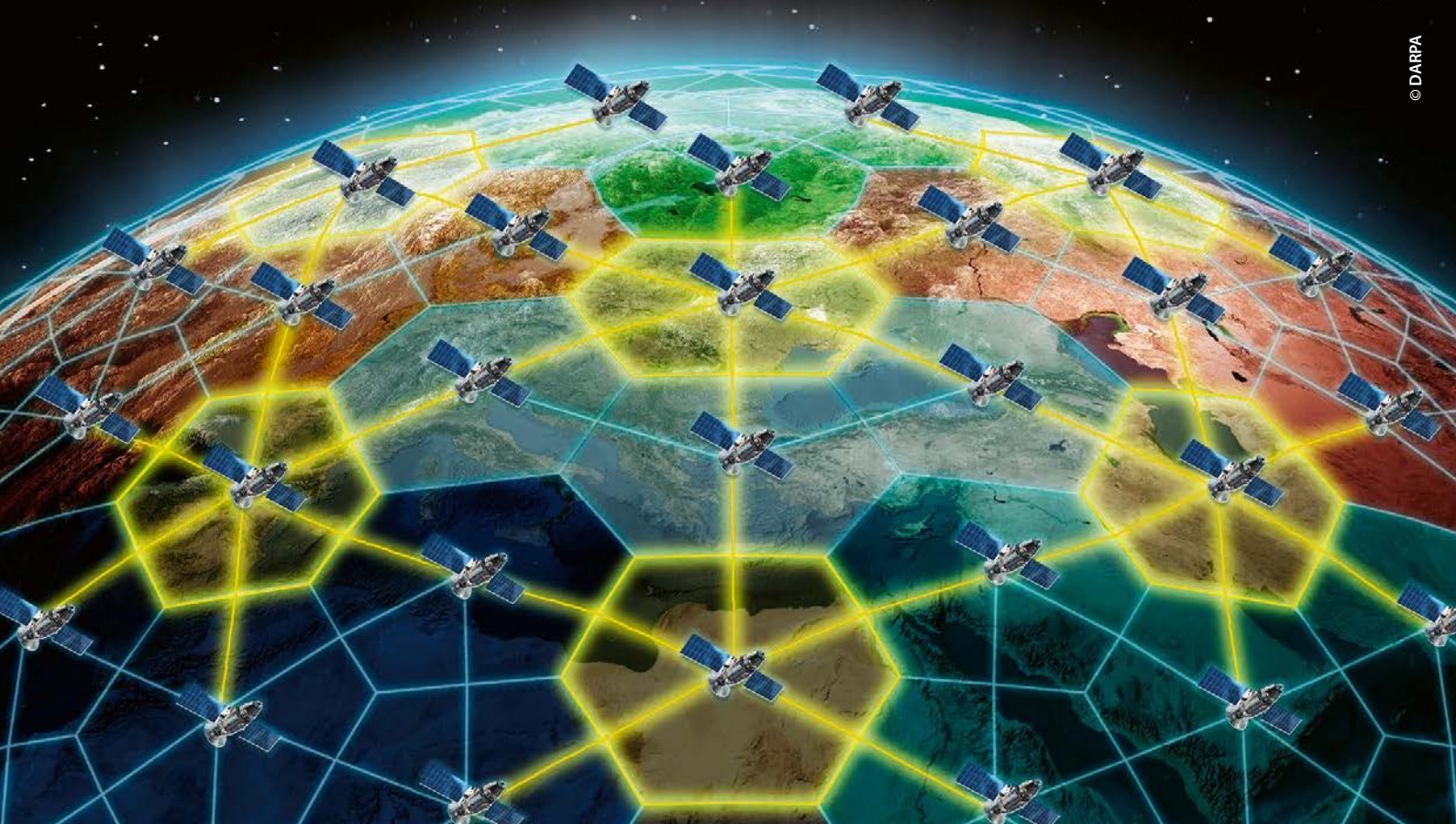
However, there is no real alternative to choosing the path of evolving our C2 systems, because potential opponents will be doing the same and thereby potentially gaining a decisive, hard-to-match advantage. Potential autocratic opponents may have far less restrictive legal and ethical boundaries for the employment of emerging technologies (e.g. AI, deep learning) and can, therefore, field these capabilities unconstrained. Hence, our system not only needs to keep up with this pace, but also needs to be capable of compensating for employment limitations with other means, allowing us to stay competitive. ●

1. Walter Perry, David Signori, John Boon, Exploring Information Superiority, 2004, https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1467.pdf (accessed 16 Aug. 2021).
2. Shannon Kempe, The Data – Information – Knowledge Cycle, Nov. 2013, <https://www.dataversity.net/the-data-information-knowledge-cycle/#> (accessed 16 Aug. 2021).
3. Andrea Ferrario, In AI We Trust Incrementally: a Multi-layer Model of Trust to Analyze Human-Artificial Intelligence Interactions, 2019, <https://link.springer.com/article/10.1007/s13347-019-00378-3> (accessed 16 Aug. 2021).
4. Artificial Intelligence, What is it and why it matters, https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html (accessed 16 Aug. 2021).
5. Big Data: The three Vs explained, <https://bigdataldn.com/intelligence/big-data-the-3-vs-explained> (accessed 16 Aug. 2021).
6. Machine Learning vs. Deep Learning, <https://datasoluto.com/machine-learning-vs-deep-learning> (accessed 16 Aug. 2021).
7. Homepage IBM, <https://www.ibm.com/quantum-computing/what-is-quantum-computing> (accessed 16 Aug. 2021).
8. Zach Hughes, Fog, Friction and thinking Machines, Mar. 2020, <https://warontherocks.com/2020/03/fog-friction-and-thinking-machines> (accessed 16 Aug. 2021).
9. Elke Schwarz, The (im)possibility of meaningful human control for lethal autonomous weapon systems, Aug. 2018, <https://blogs.icrc.org/law-and-policy/2018/08/29/im-possibility-meaningful-human-control-lethal-autonomous-weapon-systems> (accessed 16 Aug. 2021).
10. Human Rights Watch, <https://www.hrw.org/topic/arms/killer-robots> (accessed 16 Aug. 2021).
11. Bonnie Young, Future Integrated Fire Control, Jun. 2005, http://www.dodccrp.org/events/10th_ICCRTS/CD/presentations/325.pdf (accessed 16 Aug. 2021).
12. Report of the Defense Science Board Task Force on Patriot System Performance Report Summary, Jan. 2005, <https://dsb.cto.mil/reports/2000s/ADA435837.pdf> (accessed 16 Aug. 2021).
13. Dr Guy Duczynski, Effects-Based Operations: A Guide for Practitioners, <https://www.hsdll.org/?view&did=454767> (accessed 16 Aug. 2021).
14. Ibid. 4.
15. NATO Allied Joint Doctrine AJP 3 for the Conduct of Operations.
16. Katja Lindskov Jacobsen, Rune Saugmann, Optimizing Coalition Air Warfare: the Emergence and Ethical Dilemmas of Red Card Holder Teams, Jun. 2019, <https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12670> (accessed 16 Aug. 2021).
17. US Congressional Research Service, Joint All-Domain Command and Control, Mar. 2021, <https://fas.org/sgp/crs/natsec/IF11493.pdf> (accessed 16 Aug. 2021).
18. Murray Shanahan, The Technological Singularity, Aug. 2015, <https://mitpress.mit.edu/books/technological-singularity> (accessed 16 Aug. 2021).
19. Elsa B. Kania, Battlefield Singularity, Nov. 2017, <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235805&focal=none> (accessed 16 Aug. 2021).
20. Victor Rivero Diez, Spoofing and Jamming over GNSS, Jul. 2020, <https://www.incibe-cert.es/en/blog/spoofing-and-jamming-over-gnss> (accessed 16 Aug. 2021).
21. Zoltán Micskei, Robustness Testing, http://mit.bme.hu/~micskeiz/pages/robustness_testing.html (accessed 16 Aug. 2021).

Lieutenant Colonel Andreas Schmidt

joined the German Air Force in 1993. After attending Officers School, he studied Computer Science at the German Armed Forces University in Munich. Since 1998, he built up an extensive background in Ground Based Air Defence, particularly the PATRIOT weapon system. He started as a Tactical Control Officer and subsequently held positions as Reconnaissance Officer, Battery Executive Officer and Battery Commander in various PATRIOT units. Furthermore, he had two non-consecutive assignments in Fort Bliss, Texas. The main task of his first assignment was to conduct bilateral US-GE studies of weapon system behaviour on a tactical level for the German PATRIOT Office. During his second assignment, he was the Subject Matter Expert (SME) on Integrated Air and Missile Defence at the German Luftwaffe Air Defence Centre. In between, he had an assignment as the A3C in the former Air Force Division. Currently, he is the Integrated Air and Missile Defence/Ballistic Missile Defence SME in the JAPCC.





Responsive Space for NATO Operations – Part 3

By Wolfgang Jung, German Aerospace Centre (DLR)

By Dr Dirk Zimmer, German Aerospace Centre (DLR)

By Lieutenant Colonel Tim Vasen, GE AF, German Air Force HQ

Introduction

Space Support plays a significant role in modern warfare and is a key enabler for NATO's technical advantage. Worldwide technological developments challenge this advantage while Space has become increasingly congested and contested.

This is the third article of a series focusing on the Responsive Space topic. The first article was released within JAPCC Journal 31 in February 2021 and focused on definitions and international doctrinal concepts. The second article, more technically focused, was released within the JAPCC Journal 32 in August 2021.



All three articles can be accessed here:



Part 1



Part 2



Part 3

This final article will focus on potential examples of Responsive Space procedures and means for some of the Space functional areas and possible implementation options for NATO.

Responsive Space Options for the NATO Defined Space Functional Areas

Positioning, Navigation and Timing (PNT):

NATO has the chance to arrange a combination of the two Global Navigation Satellites Systems (GNSS): Global Positioning System (GPS) and Galileo.¹ Galileo can be broadly considered as the responsive means to a degraded GPS support.

Notwithstanding the positioning and navigation service of PNT systems, the timing function is specifically crucial. Losing this support element causes degradations including, for example, encrypted communication links as the synchronization relies on the timing signal to be accurate. Responsive Space means are alternative synchronization processes and procedures that ensure persistent communication links. The process could also include a navigation feature using a reference system outside the degraded PNT environment.

Intelligence, Surveillance and Reconnaissance (ISR):

Responsive launches, in response to requests or degradation, do not directly support NATO operations as they are primarily national business. In turn, those nations further supporting NATO within the overall ISR process. If the launched payload is designated, even partly, to NATO as a tasking authority, this increases its added value. Small satellites with optical, radar, or even future quantum sensor capabilities would strengthen NATO's ISR capabilities, if NATO nations were willing to share such information. Additionally, small satellites could be used for on-demand signal intelligence missions.

It should be standard practice for NATO to investigate the feasibility of utilizing more commercial support from western-based companies (NATO nations and partners) in order to increase its capacity, incorporate new capabilities, and to have a more resilient support base while relying on a wider number of legacy options.

Satellite Communications (SATCOM):

NATO should consider the integration of constellations or even mega-constellations, military or commercial,

within its communication's architecture. This will likely require hardware adjustments, but would increase communication resilience and ensure continuity of service. Outside of the Space-based communication services, there are a number of alternative solutions, such as airborne platforms, which should be explored to ensure better coverage in contested areas and to be able to close coverage gaps in case of degraded Space support services.

Space Situational Awareness and Space Weather:

It should be identified which products out of these functional areas are of the highest priority to NATO. Further exploration of which member nations can deliver these products and services allows for more resources and redundancy. This may be a chance for smaller NATO members to fill niches when they rely on additional sources for their products, such as those provided by commercial partners.

NATO Needs for Responsive Space Capabilities

As already analysed in the two previous articles, the military use of Space or the use of Space in general is vulnerable to intended counter-measures, referred to as counter-Space or Anti-Satellite Technology.² The challenge is to ensure continuous Space support to NATO. In this context, Responsive Space capabilities and procedures can be seen as elements of deterrence.³ If a potential opponent is technically able to degrade Space services, to achieve a major effect, they will need a very complex set of procedures and technically advanced equipment. If this opponent knows, from official statements and publicly released doctrine, that processes are in place to buffer their counter-space activities and restore services, then they would normally be well advised to rethink their hostile intent.

Options to Integrate Responsive Space into NATO's Operational Planning

It makes sense for NATO to know other member nations' availability of Responsive Space procedures, and

their sharing disposition. An initial step could be the voluntary establishment of a capability database detailing potential available Responsive Space means, spread over all domains. Secondly, it should be explored and agreed upon whether Responsive Space resources of a specific nation can be requested to ensure a continued support of a capability offered by the same nation. In a combined approach, it could also be possible to responsively close a capacity gap for another nation. If the combined support is then possible, a third step involving interoperability and compatibility for potential NATO use should be surveyed, as well as potential technical solutions. This approach allows bi- or multilateral solutions, strengthening the Alliance's posture, with one nation offering Space support while another provides a potential interoperable Responsive Space solution. Technical challenges, bilateral requirements and solutions can be arranged and sorted in advance.

For every Space functional area, the responsible NATO entity to request Responsive Space support has to be identified. Establishing the communication community for SATCOM or the intelligence community for ISR are options. Further, the role of the new NATO Space Centre, a key element of NATO's Space support, has also to be explored to coordinate Responsive Space actions. Establishing a network of points of contact, for the various capacities and capabilities, between the identified NATO entities and bodies to interact with the nations on the desired functional areas is of high value.

Specifically assigned or agreed policies therefore have to be included in operational planning and tested within exercises. This includes procedures on how to request Responsive Space means or actions to ensure the continued support. Deliberate exercising of corroborated responses will continuously increase knowledge and foster an environment in any headquarters for proper understanding of the related processes and procedures.

After summarizing the above Responsive Space opportunities, these should be analysed along the lines of the interdisciplinary approach, designed to be used in the Capability Development process, namely Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability (DOTMLPFI).

For NATO, in terms of Responsive Space, this could mean:

Doctrine: NATO Space Defence Strategy addressing Responsive Space as a future capability.

Organization: Space Support coordination functionality; Space Centre as core element.

Training: Education and training through common exercises (Joint Warfare Wargames) or by means of a dedicated small satellite constellation.

Materiel: Specific equipment, systems, stores, and technologies (e.g. NATO owned and ground-operated segments).

Leadership: How to make proper use of Responsive Space capability within the alliance.

Personnel: Identifying specialists and/or specific skills (e.g. NATO Space Cadre).

Facilities: Infrastructures needed to accommodate, train, and prepare (e.g. Ground and Space segments).

Interoperability: Interfaces, requirements, and standards enabling Joint All Domain Operations.

Further Research Options for NATO Bodies

NATO has the chance to integrate Responsive Space into NATO's long-term focused NATO Defence Planning Process (NDPP).⁴ By virtue of this process, NATO identifies future requirements for technical or organizational capabilities. It is preferred within NATO that the required capabilities are developed or purchased within the Alliance. Inserting Responsive Space requirements into NDPP offers the option for combined approaches leading to interoperable standardized NATO processes.

Initial steps towards NDPP involvement has been done by the NATO Science and Technology Organization (STO) and can be seen in the NATO Science and Technology Trends 2020–2040,⁵ released in 2020. Consequently, Space and Responsive Space will form the basis of a so-called 'Technology Watch Card', as well as a means to 'explore a framework for standardization and interoperability for NATO multi-domain joint operations'. Both activities support the proposal to establish a database of available systems and products, and the ongoing standardization process towards interoperability. This finally leads into research activities on how to include NATO's operational planning of the national Responsive Space means and procedures assigned to NATO.

Currently, NATO STO is investigating various aspects of Space and Responsive Space to benefit the future warfighter. The following is an excerpt of ongoing activities:⁶

- SCI-SAS-ET-058 on Alliance Space Deterrence Framework – Capabilities, Legal and Policy Analysis;
- SCI-346 on Space Risk Assessment Matrix;
- MSG-187 on Space Weather Environmental Modelling;
- SET-279 on Space-based SAR and Big Data Technologies to support NATO Operations;
- SET-274 on Cooperative Navigation in GNSS Degraded and Denied Environments;
- AVT-336 on Enabling Platform Technologies for Resilient Small Satellite Constellations for NATO Missions;

- SET-264 on Quantum Position Navigation and Timing for NATO platforms;
- IST-ET-115 on Free Space Optical Communication Networks.

As shown in the approaches before (DOTMLPFI, STO, NDPP), further research is needed by nations and NATO bodies, based on NATO requirements and across Space functional areas, to include future technologies such as Space robotics.

The increasing operational tempo requires global capabilities and near real-time availability of information across all domains. Even NATO member nations, without their own Space programmes, can contribute to resilience in Space by providing ground-based services. Both NATO and national Space security are collective activities.

Finally, the role of the Space Centre, which is defined as being 'a focal point to support NATO missions with communications and satellite imagery, share information about potential threats to satellites and coordinate our activities in this crucial domain'⁷ has to be further developed. This is essential, especially for the claimed extended responsibilities for ISR and SATCOM, where overlapping responsibilities within the intelligence and communication communities have already been identified. Furthermore, the Space Centre's role in the integration of Responsive Space means and procedures with national structures and procedures has to be explored and defined.

Overall Assessment and Conclusion

Technical developments, Space strategies and policies within the technically high-developed nations confirm the overall importance of Space and Responsive Space means within military operations. In the first two articles from this series, these topics were discussed and analysed for NATO nations and potential opponents. Based on this, NATO now has the chance, while further developing and implementing the Space domain into its processes and procedures, to embed the option to plan for Responsive Space means and procedures as a minimum. Based on the



increased reliance of military units on the availability of Space services, validated by its extensive use during military operations, NATO should identify and further explore Responsive Space options as a priority.

These may include:

- Notwithstanding the recent declaration of Space as an operational domain, NATO should identify requirements that lead to definitions on how to potentially implement Responsive Space into operational planning.
- A continuous survey of available capabilities and capacities, as already proposed by STO in the Technological Watch Card.
- Initiate discussions with member nations to make Responsive Space means and procedures available to NATO.
- Include the Responsive Space topic in the NDPP, focusing on fostering combined interoperability and

Alliance broad standards. This may include bi- or multi-lateral approaches where, for example, one nation is responsible for the Space capability and another for the specifically designed Responsive Space solution.

- Include the effects and the use of Responsive Space in NATO exercises and challenge the responsible entities.
- Deconflict potential responsibility overlaps between the intelligence and the communication communities and the Space Centre, to avoid duplications and misunderstandings.
- Analyse Responsive Space through the lens of capability development along the lines of the DOTMLPFI approach to exploit the maximum potential for NATO and its members.
- Implement Responsive Space operations into war games and identify the benefits to the warfighter.
- Support and conduct technology demonstrations for NATO and member nations to learn, adapt and act at the speed of relevance. ●

1. Tim Vasen, *Is NATO Ready for Galileo*, 2019, JAPCC Journal 28, <https://www.japcc.org/is-nato-ready-for-galileo/>, (accessed 6 April 2021).
2. US National Air and Space Intelligence Center, *Competing in Space*, 2019, Dayton Ohio, <https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF>, (accessed 6 April 2021).
3. Mike Moore, *Twilight War – The Folly of U.S. Space Dominance*, chapters 2 and 3, 2008, The Independent Institute, Oakland California USA.
4. NATO Headquarters, *NATO Defense Planning Process*, 2018, Brussels, https://www.nato.int/cps/en/natohq/topics_49202.htm, (accessed 6 April 2021).
5. NATO Science and Technology Organization, *NATO Science and Technology Trends 2020–2040*, 2020, Paris, https://www.nato.int/nato_static_f12014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf, (accessed 6 April 2021).
6. NATO Science and Technology Organization, https://www.sto.nato.int/publications/Pages/activities_results.aspx?k=space&s=Search%20Activities&start1=11, (accessed 26 May 2021).
7. NATO Allied Air Command, *NATO agrees new Space Centre at Allied Air Command*, 2020, Ramstein, https://ac.nato.int/archive/2020/NATO_Space_Centre_at_AIRCOM, (accessed 6 April 2021).

Wolfgang Jung

started as Reserve Officer for Tactical Ballistic Missiles (MGM-52 Lance), followed by two Academic Degrees (Aerospace and Space Systems Engineering). In the last 25 years at DLR's Mobile Rocket Base (MORABA), he was responsible for Launch Services and designing new Hypersonic Flight Vehicles. In 2019, he was nominated as DLR's Coordinator for Responsive Space. At the beginning of 2021, he was appointed as the Head of Technology and Department Head for Technology Demonstration at the newly established DLR Responsive Space Cluster Competence Center (RSC3). Besides this, he supports the Air Force Command in Berlin in a Reserve Officer capacity.



Dr.-Ing. Dirk Zimmer

joined the German Air Force in 2004 and holds a doctoral degree in Aerospace Engineering. Professionally trained as an ammunition specialist, he commanded a specialized maintenance unit for aerial missile systems. From 2013 to 2016, he served as Executive Officer for the Applied Vehicle Technology Panel at the NATO Science and Technology Organization. In 2019, was appointed as Executive Board Representative Defence and Security Research and, in 2020, as Managing Director to the Responsive Space Cluster Competence Center at DLR. Furthermore, he is a Member of the Science and Technology Board and is an advisor to the FMod and the Munich Security Conference.

Lieutenant Colonel Tim Vasen DipEng, MSc

served for several years in commanding and staff positions within the artillery branch, including a deployment to KFOR as company commander of the DEU ISTAR-company before becoming a career intelligence officer. Serving 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). From October 2017 until August 2021 he was a member of JAPCC, responsible for Space Intelligence. In August 2021 he joined the German Air Force HQ, responsible for Space Intelligence development.



Potential Game Changer for Close Air Support

Enhancing UAS Role in Contested Environments

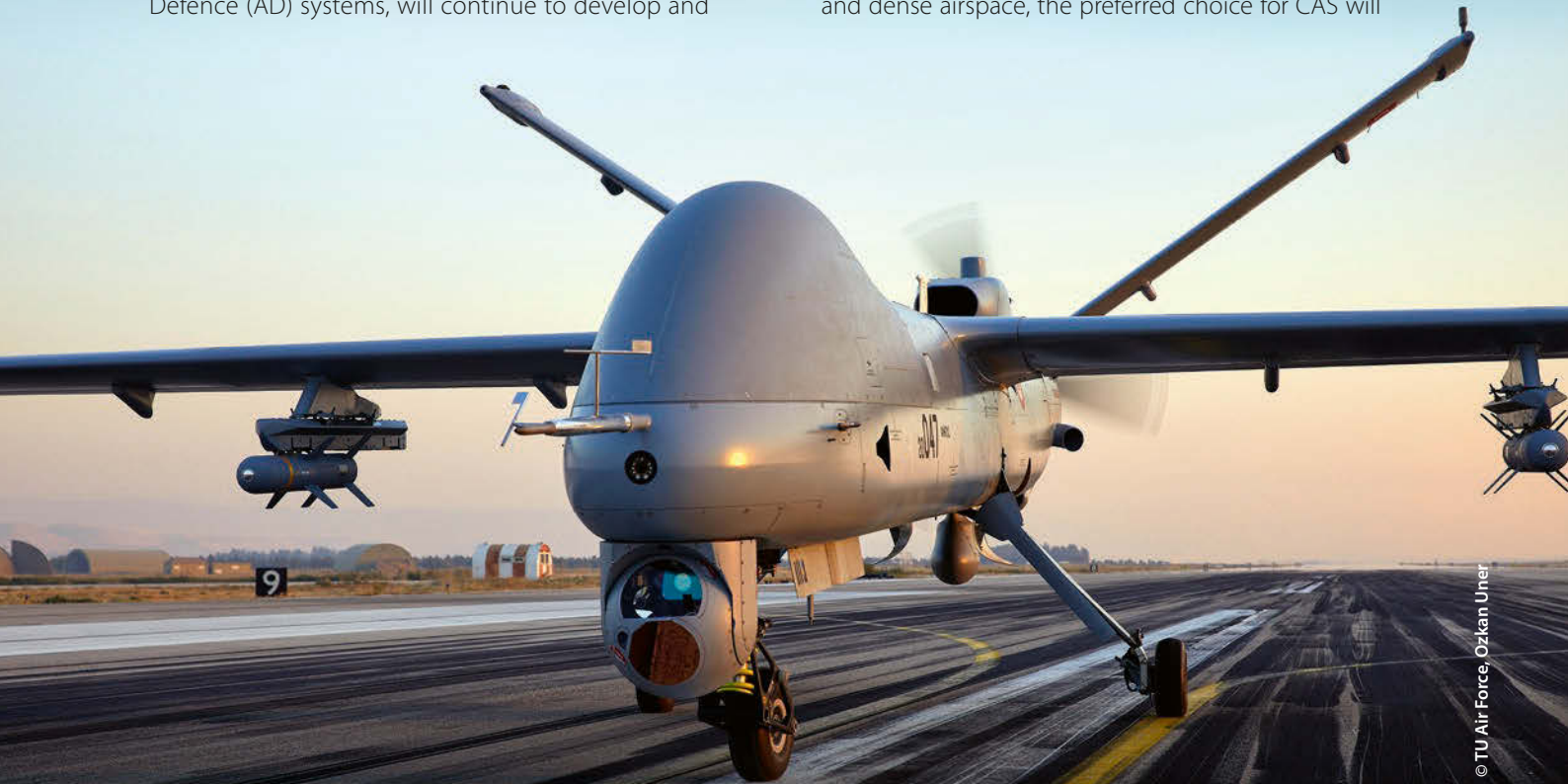
By Lieutenant Colonel Osman Aksu, TU AF, JAPCC

Introduction

The NATO Strategic Foresight Analysis¹ provides a projection of the world's strategic trends up to and beyond 2035. It predicts that asymmetric conflict scenarios will continue and that the need for collective defence against a peer or near-peer adversary will be increasingly likely. In addition, difficult, urbanized conflicts are also a probable challenge for the future, and both are likely to require modification of the Alliance's current Close Air Support (CAS) operations model.² Providing CAS to joint forces remains a crucial mission in the context of joint force operations. However, peer adversary capabilities, including the threat posed to Alliance platforms from Air Defence (AD) systems, will continue to develop and

increase in lethality at a relentless pace. The period of uncontested operating environments is now replaced by the new paradigm of contested environments defended by adversary Anti-Access/Area Denial (A2/AD) capabilities.

Before CAS operations commence, decision-makers must weigh the effects of different airframe capabilities against critical and sensitive ground targets, while balancing friendly ground forces survivability. The allocated CAS airframes should meet the conditions for effective CAS, while minimizing vulnerability to sophisticated adversary AD systems. CAS operations will have to be effective in both non-peer and peer-level engagements/environments. In high-threat conflicts and dense airspace, the preferred choice for CAS will



be multi-role 5th generation aircraft. In the aforementioned scenario, requesting dedicated CAS assets in order to effectively fulfil CAS requirements, while at the same time only being able to employ scarce, highly capable multi-role platforms in the CAS role due to issues of survivability is a dilemma.

Recent operations have demonstrated that Unmanned Aircraft Systems (UAS) can deliver precise effects in space and time and, therefore, could be utilized in close proximity to both friendly forces and, if necessary, non-combatants/civilians. This article intends to describe how UAS can support CAS missions and raises the question whether they might be the platform of choice for future CAS operations. In 2014, a JAPCC study³ focused on the use of UAS in possible future combat environments where an adversary's defences pose a threat that could be higher than that seen in earlier military operations. Enhanced survivability options were explicitly defined, and the study presented more than 100 recommendations. Within this paper, some evaluations are made in light of this earlier study's opinions, recommendations, and lessons identified in recent military operations.

The Role of UAS in CAS Operations

UAS are already playing a critical role on the battlefield and provide distinct capabilities to the warfighter. These capabilities include Intelligence, Surveillance and Reconnaissance (ISR) and precision targeting during combat operations. UAS can loiter over suspected or known adversary strongholds, mostly in uncontested environments, to locate, monitor, and, if necessary, engage targets of opportunity for long periods. Now that more enhanced features are incorporated into UAS, such as carrying guided air-to-ground munitions, stealth features, or Electronic Warfare (EW) packages, these systems are touted as the future of air combat vehicles. Ideally, these capabilities would classify UAS as prime candidates for CAS opportunities. UAS have developed into vital CAS tools and are no longer considered solely an ISR asset.

Airspace Access

Some degree of control of the airspace over the battlefield is a prerequisite for CAS sorties to be flown in support of friendly ground troops. UAS are not traditionally



AKINCI is the latest culmination of the company's drone development projects.

intended to operate in highly contested airspace where even localized access is impractical. However, in a situation where sending manned aircraft into contested airspace would pose a significantly higher risk, UAS may offer an alternative. While UAS still face risks from enemy defences, they may be based closer to the front lines, allowing for faster response and longer loiter times in support of ground operations while having a zero-risk level for aircrews.⁴ Effective airspace control measures reduce the risk of fratricide, enhance UAS survivability, increase flexibility, and can strengthen UAS CAS operations.

A safe flight routing to their area of operations is paramount for UAS. If the adversary AD measures are significant, air support from UAS might be limited until the threat is reduced or neutralized. Modern UAS can fly in pre-planned airspace with precisely defined limits, thanks to the introduction of advanced systems and sensors such as redundant navigation and Satellite Communication (SATCOM) capabilities. New navigation and control technologies, coupled with the ability of modern UAS to carry more on-board sensors, have significantly improved UAS CAS capabilities. Additionally, improved stealth features, enhanced counter-measures capabilities,^{5,6} and the ability to have buddy drones or small-sized UAS (such as Harpy)⁷ to execute Suppression of Enemy Air Defences (SEAD) are extremely valuable in the modern-day battlespace. These can contribute towards achieving commanders' goals before the CAS mission even commences and be a game-changer in a close fight. Despite a payload capacity in large-sized UAS that allows for the carriage of multiple SEAD weapons, their size creates a vulnerability that may well make these missions quite challenging. Stand-off jamming and decoy drones might very well be essential enablers for use against integrated AD systems.⁸

With the above scenario, the logical solution is a hybrid UAS/manned Combined Air Operations package to give redundancy, safety in numbers, and the collective protection of assets. It would seem unlikely that, alone, UAS could be an effective substitute for manned fighters, but when the situation is dire, the alternative is to launch drones with enhanced capabilities to achieve mission objectives.

An example of this type of scenario was displayed during the Azerbaijan and Armenian conflicts, where the Azerbaijani's drone-led assault seemed to have scored a decisive victory over Armenian AD in the disputed enclave of Nagorno-Karabakh.^{9,10} 'KARGU' smaller tactical kamikaze drones, designed for use against static or moving targets, were employed and with the help of the latest enhancements easily overwhelmed their targets.^{11,12} Swarm UAS are relatively cheap, expendable, and designed to operate together in large numbers; forming a swarm to overwhelm the adversary's defences and achieve the desired military effect. These are thought to be the systems of choice for the most 'dull, dirty, or dangerous tasks'.¹³ Effective use of UAS swarms in contested airspace will be crucial in guaranteeing the airspace access requirement, which is vital for CAS, especially by permanently neutralizing local adversary AD capabilities or, at least, for a defined period of time.

Integration

The integration of UAS into CAS operations requires detailed mission planning, including UAS operators' recommendations regarding tactical UAS situations, capabilities, and contingency procedures. Understanding UAS's unique capabilities and the current tactical situation will support achieving the desired effects. Today, since most NATO nations own modern UAS, there are minimal problems foreseen in understanding capabilities. However, addressing UAS CAS planning considerations (such as communications capabilities, payload status, contingency procedures, airspace deconfliction) is crucial for each service before operations commence. An increased emphasis on UAS Tactics, Techniques and Procedures in CAS training will further increase the existing synergy between services. A consideration, at this stage, that would also increase coordination and save time is to develop options for having interconnectivity or machine-to-machine interface in the communications network between elements in the CAS system.

Command and Control

CAS Command and Control (C2) requires a safe, dependable, and interoperable communications system



between aircrews, air control agencies, Joint Terminal Attack Controllers/Forward Air Controllers, ground forces, and fire support agencies. From a CAS standpoint, sensor and communications suites represent the system's heart and soul and ultimately determine whether UAS are compatible with CAS missions. On the battlefield, peer adversaries or non-state actors can specifically jam Global Positioning System (GPS) receivers and data links, having a significant negative impact on the operational use of UAS. A new generation of SATCOM features facilitates the UAS's potential role as a communications hub in the C2 network, assists with multi-domain operations, and, perhaps, reduces the likelihood of effective jamming or interference. UAS with radio relay capabilities in the different frequency bands (Ku, C band in Line of Sight [LOS] operations) can play a life-saving role, especially in contested environments. Some UAS upgrade programmes (like with the MQ-9 Block 5) are underway to enhance their communication capabilities in contested or remote environments.¹⁴

Other than the technological mitigations for challenged C2, the next best option might be to execute distributed control of critical air missions when needed. Creating more C2 nodes and handing over more responsibilities to subordinates via mission-type orders can help achieve a commander's intent.¹⁵ In time-

constrained and contested environments, the strike decision might need to be made closer to the source of target detection, like from a UAS, with the help of subordinate Tactical C2.

Accuracy

Firepower is the livelihood of CAS platforms, and it must retain accuracy under enemy fire. Accuracy is paramount to prevent fratricide and to limit the risk of collateral damage. The increasing array of UAS weapons is vital on the battlefield, providing a variety of options for planners. The MQ-9's laser-guided munitions and missiles, supplemented by the addition of a synthetic aperture radar to enable future GBU-38 Joint Direct Attack Munitions targeting, is a good example of fielded enhancements to modern UAS.¹⁶ It is anticipated that new technology, such as the GBU-53B SDB II carried by UAS like the Predator C Avenger,^{17,18} will have a positive impact on weapon performance with redundant built-in features like a tri-mode seeker to ensure accuracy, especially in an environment where GPS signals can be compromised.

Responsiveness and Timeliness

The responsiveness of Air Power is crucial for ground forces' survivability, and it often affects their scheme of



The ANKA-S has been used by the Turkish Air Force for more than five years in critical air operations.

manoeuvre. Timely target acquisition is fundamental to effective and responsive CAS. UAS sensor capabilities are an essential factor for target acquisition to pinpoint enemy locations and to discriminate them from friendly troops and civilians. Longer loiter times over areas of interest with enhanced target acquisition capabilities can make UAS more valuable during operations. To further improve CAS responsiveness, the deployment of UAS to forward operating locations inside a friendly theatre provides for decreased response times and rapid movement into its Area of Operations with sustainable logistic support, including rearming and refuelling, increased loiter time, and the maintenance of UAS on alert status, which are all critical factors for consideration. To enable quick targeting decision-making and to allow delegation to the lowest possible level within engagement authority and accomplish effective CAS, air planners must have timely and accurate intelligence data regarding the enemy's capabilities and locations to make informed decisions.

Survivability

Defined as 'The capability of a system to avoid or withstand hostile environments',¹⁹ Combat Survivability is the most significant parameter to consider when deciding whether a UAS role in CAS is sustainable.

Although new UAS weapons and communications technologies bring enabler capabilities to the battlefield, UAS still have considerable limitations, such as the lack of stealth and reduced speed or manoeuvrability. Any UAS that heads into capably defended adversary airspace needs to be able to counter powerfully integrated surface-based AD systems, EW, combat aircraft, and Man Portable Air Defence Systems. The ability to cope with these threats will determine the attrition rate of UAS in such an environment. Enhancing the combat survivability of UAS is required to make them fit for purpose in a CAS scenario. This requirement depends on many factors such as the mission, the threat environment, the number of available UAS executing missions, payload capability, or potential alternative capabilities. Future UAS will need reduced radar cross-sections, threat detection and avoidance (active self-defence), damage tolerance, improved autonomous functionality, and redundant navigation system capabilities to survive in a contested environment. Reliable intelligence and detailed mission planning (unpredictable or variable flight paths) of the UAS operation will positively affect survivability. The combat survivability of a particular UAS will weigh heavily on the commander's decision whether to integrate it into operations. There must be a balance between combat survivability, mission performance, and reliability.



TB2-BAYRAKTAR: More than 400,000 flight hours in Turkish Armed Forces.

Example of Tactical UAS Operation in a Contested Environment

Each conflict and its dynamics are different, and the operations in which friendly forces carry out missions must be shaped accordingly to the operations area. During Operation Spring Shield (2020), in Idlib, Syria, the airspace was highly contested, and friendly communications were heavily disrupted. Despite these unfavourable conditions, providing CAS and safety for ground troops was an urgent priority and local commanders had limited options. The best option was to access the operations area with intensive EW support (especially against high GPS jamming) and hit predetermined or dynamic targets using detailed intelligence information verified by friendly ground forces. The definitive solution was to pierce the contested airspace bubble. However, the critical question was which assets could provide the needed effects? The correct response with a timely, accurate, and massive standoff attack could be more important than to risk losing assets by entering into the denied airspace with minimal communications capability. Turkey used armed UAS as the primary element in Idlib (2020) and Libya (2019–2020).²⁰ Having a larger

payload capacity, extended loiter time, redundant navigation features against GPS jamming, and being part of a resilient digital communications network among all services gave the satellite-linked ANKA-S a distinct advantage during the operations in Idlib. Over the battlefield, the ANKA-S flew in squadrons, which were able to 'Swarm' and overwhelm AD systems, quickly nullifying that defensive capability.²¹ Based on the available options, the commander decided to send a massive coordinated UAS force rather than manned aircraft, which could be lost and the pilots killed, with the potential attrition negatively impacting the remaining friendly military capabilities. These technological and tactical developments of ANKA-S employment have improved overall combat survivability, without active or passive defences against air-to-air attacks or ground-based AD, as well as in adverse weather conditions.

Going Forward

UAS technology is rapidly maturing and becoming the multi-role superstar of future combat operations. By leveraging their endurance capability and amassed

firepower, UAS technology can provide timely and responsive CAS for operations. Detailed planning is critical to integrating UAS into CAS operations and requires a thorough understanding of the specific UAS capabilities and vulnerabilities to make sound tactical recommendations. There also exists a requirement for well-trained personnel, grounded in UAS operational concepts, to harmonize the tactics in contested environments. UAS are aptly suited for ISR and the attack of dynamic targets, and they can be critical in winning the battle by considering valid operational tactics and combat support planning. UAS need enhanced survival systems, if missions require them to operate in contested areas. However, not possessing the enhanced survivability equipment of manned aircraft and having speed and manoeuvre limitations as comparable to manned aircraft; these vulnerabilities inside contested environments are still an issue until new cutting-edge UAS technologies such as Unmanned Combat Aerial Vehicle with stealth and greater manoeuvrability will be centre stage in the battlespace.²² The standard 'one-size-fits-all' solution will not always be available, and decision-makers should explicitly balance UAS roles during operations versus the risk of their loss in high-threat areas. Digesting lessons learned from past air campaigns in geopolitically sensitive and risky areas will be crucial to enhancing UAS survivability in future conflicts. ●

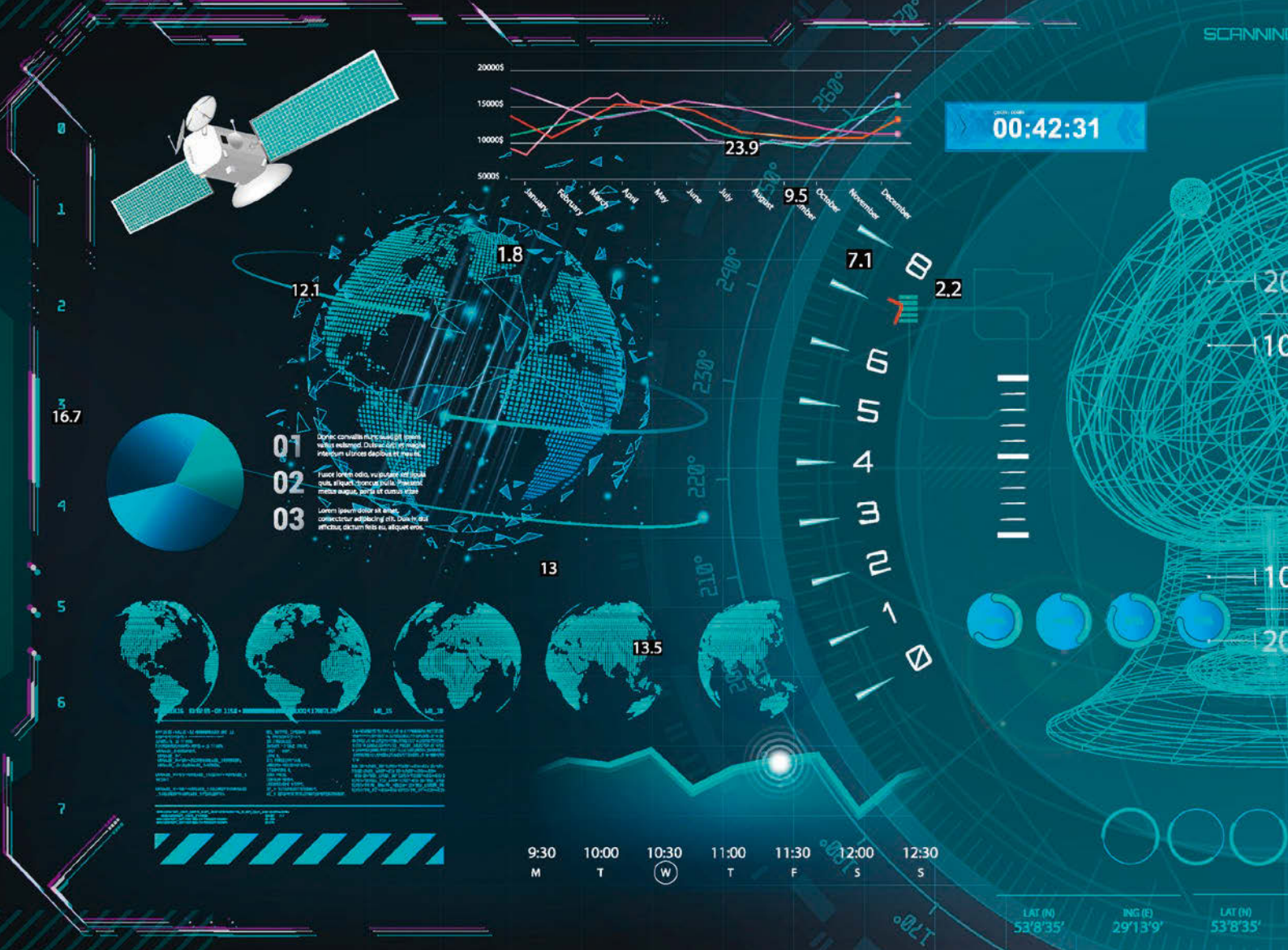
'The future is in the skies.'
Mustafa Kemal Atatürk

1. NATO Supreme Allied Commander Transformation (SACT), 'Strategic Foresight Analysis', 2017.
2. D. Cochran, A. Haider, and P. Stathopoulos, Reshaping Close Support Transitioning from Close Air Support to Close Joint Support, JAPCC, 2020.
3. A. Haider, Remotely Piloted Aircraft Systems in Contested Environments, JAPCC, 2014.
4. T. Phillips-Levine, D. Phillips-Levine, W. Mills, <https://mwi.usma.edu>, 7 January 2020, <https://mwi.usma.edu/unmanned-lethal-organic-future-air-support-ground-combat-forces/>.
5. General Atomics Aeronautical, <https://www.ga-asi.com/multi-mission-payloads>, (accessed 15 October 2021).
6. G. Reim, <https://www.flightglobal.com/military-uavs/record-number-of-uav-shoot-downs-prompt-new-usaf-tactics-and-countermeasure-pod/138908.article>, (accessed 10 March 2021).
7. I. A. Industries, <https://www.iai.co.il/p/harpy>, (accessed 10 March 2021).
8. M. G. James Poss, 'Inside Unmanned Systems', <https://insideunmannedsystems.com/unmanned-warfare-stuff-just-got-real/>, (accessed 15 October 2021).
9. D. Barrie and N. Ebert, <https://www.iiss.org/blogs/military-balance/2021/07/nagorno-karabakh-armed-uavs>, (accessed 15 October 2021).
10. K. Fahim, 29 November 2020, https://www.washingtonpost.com/world/middle_east/turkey-drones-libya-nagorno-karabakh/2020/11/29/d8c98b96-29de-11eb-9c21-3cc501d0981f_story.html, (accessed 15 October 2021).
11. P. Iddon, 4 October 2020, <https://www.forbes.com/sites/pauliddon/2020/10/04/turkeys-drones-are-coming-in-all-sizes-these-days/?sh=10ccc1cf2004>, (accessed 15 October 2021).
12. J. Zitser, 30 May 2021, <https://www.businessinsider.com/killer-drone-hunted-down-human-target-without-being-told-un-2021-5?r=DE&IR=T>, (accessed 15 October 2021).
13. Ibid. 3.
14. J. Keller, 17 May 2018, <https://www.militaryaerospace.com/computers/article/16726910/air-force-asks-general-atomics-to-upgrade-122-mq9-block-5-reaper-unmanned-attack-drones>, (accessed 15 October 2021).
15. N. J. Hall, Preparing For Contested War: Improving Command And Control Of Dynamic Targeting, Air University.
16. <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/>, (accessed 15 October 2021).
17. General Atomics Aeronautical, <https://www.ga-asi.com/remotely-piloted-aircraft/predator-c-avenger>, (accessed 15 October 2021).
18. Raytheon Company, Missiles Systems, Air Warfare Systems, https://www.airforcemag.com/PDF/SiteCollectionDocuments/Reports/2010/August%202010/Day25/SDBII_factsheet_0810.pdf, (accessed 7 April 2021).
19. R. E. Ball, The Fundamentals of Aircraft Combat Survivability Analysis and Design, American Institute of Aeronautics and Astronautics, Inc., 2003.
20. J. Pack and W. Pusztai, 'Turning The Tide, How Turkey Won the War for Tripoli', p. 12–13, Middle East Institute, 2020.
21. A. Gatopoulos, 3 March 2020, <https://www.aljazeera.com/news/2020/3/3/battle-for-idlib-turkeys-drones-and-a-new-way-of-war>, (accessed 11 March 2020).
22. Baykar Defence, 23 April 2021, <https://baykardefence.com/haber-Turkeys-Akinci-UCAV-successfully-hits-targets-with-Roketsan-munitions.html>, (accessed 11 May 2021).

Lieutenant Colonel Osman Aksu

graduated in 2001 from the TURAF Academy with an Electronic Engineering Degree. After undertaking flight training and basic Weapons Controller training in İzmir, until 2003, was assigned as Weapons Controller at Diyarbakır CRC. In 2008, he was selected as AEWG Project Officer for Peace Eagle in the US, returning to TURAF HQ Ops Div in 2010, working as PE Project Officer until 2013. In 2013 was selected as Weapons Controller at NAEW FC GK and, in 2014, Fighter Allocator at CRC Ankara. Between 2014 and 2019, while assigned as Airspace Coordination Officer in ATC Ankara, participated in Airspace Control-Management activities for US/Coalition OIR missions. In November 2019, Lieutenant Colonel Aksu became the SME for CAS/JTAC in the CA Branch of the JAPCC.





Space Domain: A Global Vision

By Dr Massimo Claudio Comparini, Chief Executive Officer, Thales Alenia Space Italy

Space technologies moved fast in the last decade. Enhanced and new technologies combined with a business-model evolution enabled the conception and realization of a new class of space assets, which addressed new challenges and more sophisticated needs of the global user community. If the technology evolution transverses civil and military domains, the construction of specific assets for the Ministries of Defence and military users remains very important; at the same time we cannot ignore the new wave of commercial systems. Global surveillance with its persistent or quasi-persistent capabilities, global space connectivity with next-generation broadband hybrid

networks, protection to counter cyber threats, the capability to protect assets in orbit and accomplish orbital maintenance combined with the ability to operate following military doctrine in the space domain, all require effective technological and architectural solutions, potentially derived from commercial markets.

This challenge is particularly relevant considering that, in the past few years, space and cyberspace have moved from 'key enablers' to a recognized position as domains, alongside the 'traditional' domains. An extraordinary revolution. For more than a century, there were three domains of operations: land, mari-

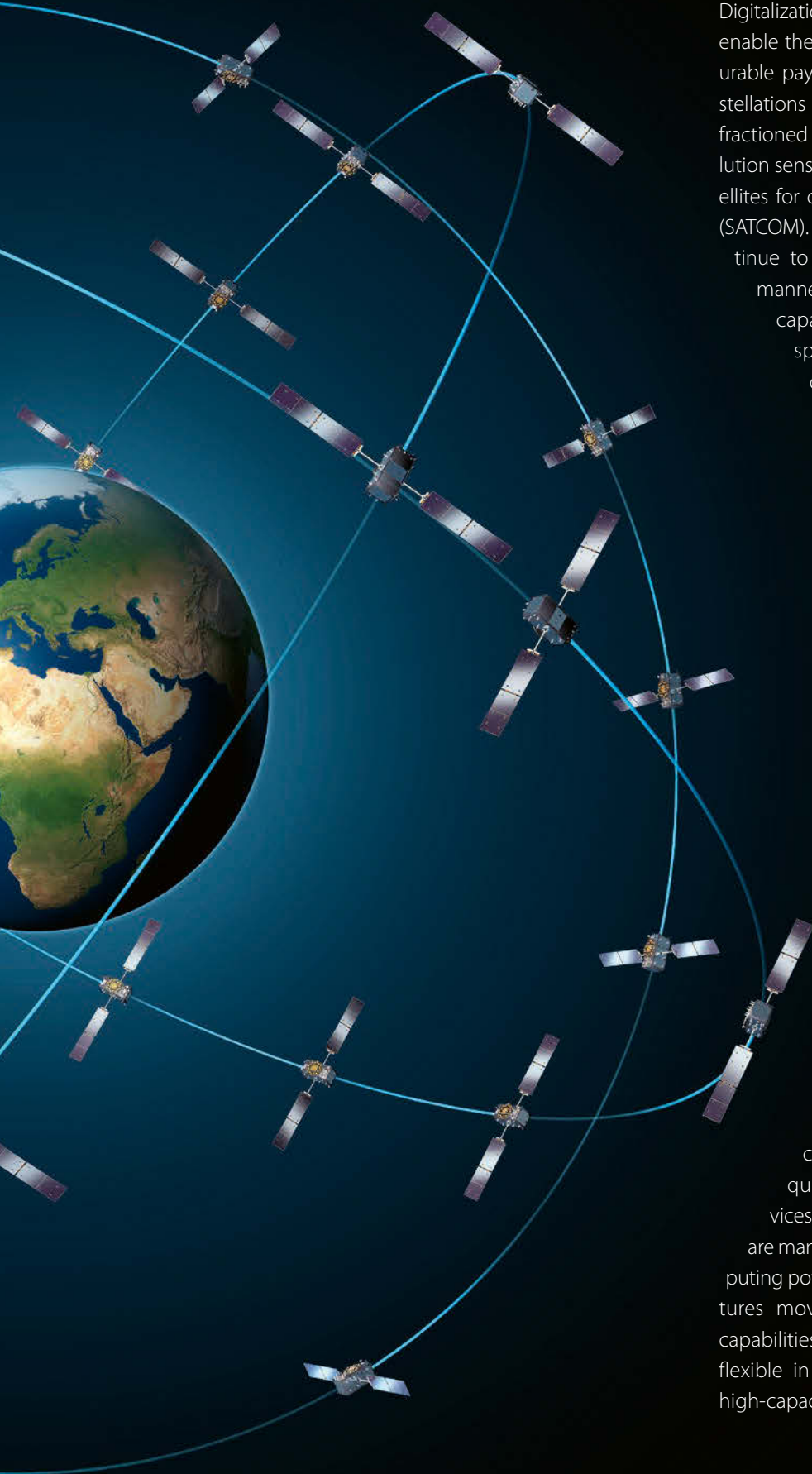


time, and air. Now, in less than three years, NATO has added two new domains, Cyber in 2016 and Space at the end of 2019. This will radically change the whole concept of military operations and warfare. The impact of space and cyberspace must be considered in the framing of the definition of multi-domain operations, capturing the ability to use information-enabled command structures and combat capabilities to build information security across the full array of domains.

Without a doubt, a day without space will severely degrade not only NATO, but also every country's capability to operate and defend. Space is essential to supporting modern military operations in a complex, multidimensional, highly dynamic and disruptive environment. It is essential to a coherent Alliance deterrence and defence posture. The information gathered and delivered through satellites is critical to all NATO

activities, operations, and missions. The role of space to conduct Intelligence, Surveillance and Reconnaissance (ISR), support missile defence, provide Position, Navigation and Timing (PNT), and facilitate tactical operations in the other domains is essential. Space is crucial to providing commanders with situational awareness, accurate assessments, and maintaining real-time or near-real-time information superiority to support fast decision-making.

Similar to the missions in the air domain, the space domain will see the emergence of new missions and operational concepts from space superiority to space dominance, defensive and offensive counter-space, space surveillance and tracking, or debris removal. Even though NATO has pledged not to 'weaponize' space, this pledge does not guarantee that other players will apply similar self-restraint. NATO needs to be ready.



Emerging space technologies offer vast opportunities. Digitalization and miniaturization of onboard systems enable the construction of next-generation reconfigurable payloads and satellites, including global constellations and mega-constellations, federated and fractioned space infrastructures, extremely high-resolution sensors and tremendously high-bandwidth satellites for civil and military Satellite Communications (SATCOM). Additionally, spacefaring nations will continue to promulgate reusable and manoeuvrable manned and unmanned spacecraft and vehicles capable of operating in lower sub-orbital space. Concurrently, space is becoming more crowded and competitive with some countries having developed and tested a wide range of counter-space technologies requiring NATO countries to maintain the state-of-the-art in this domain.

SATCOM

The space segment of SATCOM is a major contributor to secure end-to-end connectivity and is a key requirement for any in-the-field operation and for future combat air systems, as part of a much larger System of Systems (SoS). Concepts such as the United States Air Force's Advanced Battle Management System (ABMS) are indicative of the future of these SoS, including a robust space element. The amount of protected or classified information to be shared among forces is exponentially increasing and the data accessing and processing capabilities become true game-changers. To cope with the flexibility requirements and to offer advanced new services, digital and reconfigurable in-orbit solutions are mandatory. The improvement in on-board computing power makes it possible to conceive architectures moving from the standard reconfiguration capabilities to fully software-defined payloads, ultra-flexible in both frequency and coverage, for very high-capacity geostationary satellites.

At the same time, global coverage necessitates new Low Earth Orbit (LEO) constellations based on low-latency solutions. For the past few years, the commercial market has aggressively explored these solutions and now NATO must consider the advantages offered to military users. The end-goal for military and NATO requirements combines the expected evolution of requirements with the need to share in multinational/coalition operations and networks resulting in a multi-layered constellation architecture.

ISR

The evolution of Earth Observation (EO) capabilities from space and the geospatial information domain is a central part of a global digital transformation process to secure information superiority. NATO has increasingly delivered more information through geospatial data and services. The combination of EO data and data coming from a wide array of platforms, including media streams (i.e. open-source intelligence), is a fundamental part in this digitalization revolution.

NATO must anticipate the exponential growth of the impact of Information Technology (IT), advanced algorithms, machine and deep learning, and Artificial Intelligence (AI) to generate information streams for a range of user communities. These changes will certainly affect military users, with requirements to specifically address change detection, near-continuous monitoring, and persistent or quasi-persistent surveillance. In conjunction with cloud-based large computational capabilities, space and digital technologies are the fuel for the engine driving the transformation in the geospatial sector and represent a real game changer in the geospatial sector for military exploitation.

Even if large or mega-constellations of small/micro-satellites are limited in resolution, they offer the advantage of high-revisit rates and high resiliency of the whole architecture, providing continuous flow of data in optical, radar, multi-spectral, electromagnetic radiation sensing and Signals Intelligence (SIGINT) data. These systems are essential to build true patterns of life, to quickly identify what is changing on earth, both globally and locally.



Missile Defence

To defend against new threats such as hypersonic missiles and to detect and track manoeuvring high-speed missiles, space-based capabilities can undertake missions currently carried out by manned and unmanned aircraft. As an example, space constellations offer accurate Moving Target Indicator (MTI) capabilities against different categories of targets. In combination with navigation and positioning data and data generated by aerial platforms (drones, High Altitude Pseudo Satellites (HAPS), low suborbital vehicles, etc.), these constellations provide true dynamic analytic capabilities through multi-sensor and multi-platform real-time data fusion.

Data-Driven Decision-Making

Data-driven decision-making, which means AI-based learning techniques combined with big data analytics, provides warfighters at each level with the actionable information that helps them make data-informed critical decisions in real time. The ability to analyse, coordinate, and fuse massive amounts of raw data depends heavily on the available computing power, data storage capability, and power constraints. The key to success will be to synchronize operations and intelligence by continuous exploitation of analysed data in the Processing, Exploitation and Dissemination (PED) cycle.



These brief highlights already give the idea of how space domain and its convergence with cyberspace and the digital world is relevant for the Alliance. The Internet of Things (IoT) or, in this case, the Internet of 'Military' Things will produce a huge amount of data generated by space systems, sensors, and device nodes. To address the need for decisions at the speed of relevance, exponential computing power, cloud platforms, edge-computing nodes, and the big data dimension requires NATO to explore and exploit the concept of Digital Continuum¹ into the multi-level structured space domain to deliver a fast and continuous flow of information.

Until now, NATO has kept a traditional distinction between space companies, space technologies, and IT companies. In the future, NATO needs a combination of all those industries to implement effectively those space capabilities required to generate and assure information superiority of all Alliance countries and to gain advantage, in terms of both speed and capability, and to evolve the business paradigm.

How to Protect Space Assets?

Today, space systems are essential for our economies, the security of our countries, our information superiority, and subsequently for effective command and control, missile defence, early warning, and ISR. These space systems represent critical infrastructure requiring protection, especially given the exponential growth and congestion of LEO. From the more than 4,000 active satellites today, we will reach an estimated 50,000 by the end of this decade, for an entire space economy of more than one trillion USD.

In this setting, Space Traffic Management (STM) rapidly becomes a priority topic in space policy, protecting space infrastructure and guaranteeing the safe and sustainable use of outer space in the long term. Military stakeholders must consider challenges and opportunities associated with STM and become engaged in the debate to assess and influence how a changing environment may affect military space operations and space support to operations. Space Situational Awareness (SSA) is essential to manage the increased traffic and to avoid and prevent disruptive collisions in orbit.

The Role of In-Orbit Services (IOS)

Despite the difficulty in developing a comprehensive definition, IOS provide a number of actions including, but not limited to, maintenance, tugging, and inspection. Relevant examples of IOS are the reconfiguration of spacecraft payload or modules, station-keeping docking of the service spacecraft with a target satellite, orbit correction to include relocating space systems to the required orbit, creation of large infrastructure in orbit that cannot be assembled before launch due to their weight, volume, size, etc. In any case, IOS require rendezvous and close proximity operations, which could be defined as *orbital manoeuvres in which two spacecraft arrive at the same orbit and approach at a close distance*. Close proximity operations usually imply two space systems within a few kilometres or less from each other. IOS provides capabilities that will enable a range of activities to include space safety, space security, and certainly military operations, both defensive and offensive.

IOS will also require better SSA to be operational, most likely resulting in enhanced debris management and active debris removal. These elements are ideal for cooperation across borders, between national Space Commands, and for a possible specific analysis from NATO.

Conclusion

Having superficially highlighted a few relevant elements, it is useful to debate how space assets and space technologies may contribute to respond to the capability needs of NATO today and in the future. We need to increase resiliency and survivability of our space assets, including 'hardened' ground and launch capabilities, with a combination of passive and active solutions maintaining the ability to manoeuvre in the space domain to assure our missions.

Resiliency of space support, defined as 'the ability of a space system architecture to ensure a persistent support to mission success in spite of hostile actions',² is the priority. Firstly, we must deter the enemy from detecting and targeting space services or assets. Then, we must assure the ability to reconstitute, either by launching new assets or activating spare capabilities, in-orbit or ground-based. NATO requires the architectural and technological capabilities to conceive and support higher resiliency in space missions through disaggregation, distribution, diversification, protection, proliferation, and deception of space assets.

A number of enabling technologies are essential to provide a new dimension of information superiority from quantum communication to persistent surveillance and from AI-based advanced information algorithms to space robotics. A systemic and holistic approach will be essential to utilize the benefits of the technology evolution and to rapidly incorporate new integrated architectures while simultaneously building proper technology planning capacity road maps. The Alliance must protect the entire value and supply chain at governmental/institutional/industrial levels during the process to grow technological readiness levels. A multinational coordinated and cooperative effort in this respect can be very effective and NATO may play a large role in this regard.

In conclusion, to be effective in the new space domain, our countries must share a principle of cooperation at the political and technological levels in conjunction with an evolution of the standard paradigms in the public-private partnership. The role of transnational organizations, industries, and, of course, NATO, together with the capability to build up cross-border partnerships are fundamental to responding to the challenges facing our Alliance. ●

1. Digital Continuum framework: a conceptual model anchored at one end by Digital Products and at the other by Digital Services.
2. Space Domain Mission Assurance: A Resilience Taxonomy, A White Paper, Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, September 2015.



Massimo Claudio Comparini

holds a Master Degree in Electrical Engineering, Remote Sensing and Radar Systems, University of Rome La Sapienza (Italy), and a Degree in Strategy from Graduate School of Business, Stanford University, CA (USA). He is currently Deputy Chief Executive Officer of Thales Alenia Space Joint Venture, SEVP Observation, Exploration and Navigation and Chief Executive Officer of Thales Alenia Space Italy. He started his career in 1983 at Selenia Spazio (later Alenia Spazio), holding various management positions, up to the role of Chief Technology Officer. In 2013 he was appointed Chief Technical Officer of Telespazio. In 2016 he became the CEO of e-Geos, a JV company between Italian Space Agency and Telespazio, established global leader in the Earth Observation and Geo-Spatial Information and Director Line of Business Geo Information at Telespazio. He was Chairman of the Board of GAF (Germany) and EarthLab Luxembourg, still in the geospatial business domain. In his long career he held a number of academic chairs in technical, economics and innovation management disciplines, while also a member of various academic and scientific boards.

Meeting the Needs of Future Warfare

The JAPCC's Experience as a Provider of an Opposing Forces (OPFOR) Element for NATO Exercises

By Lieutenant Colonel (ret.) Ed Wijninga, NE AF, JAPCC

In the first two decades following the end of the Cold War, NATO and its member states focused their training and exercises on the immediate needs of the new and diverse demands of crisis management operations. These demands were in many ways very different from what NATO had been preparing for in the 1970s and 1980s, and therefore required a considerable refocusing of education and training, i.e. the knowledge to be acquired and the skills to be trained at the tactical level, but even more so at the operational and strategic levels.

inception, both have fulfilled exactly the needs of the time, focussing on Crisis Response Management and Counter-Insurgency Operations. The emphasis on training at the JWC was at the operational and strategic levels, while at the JFTC it was at the tactical level. The role of Air Power in these types of scenarios was quite limited, mostly focussing on the transport and the Intelligence, Surveillance and Reconnaissance

Shifting the Focus of Training and Exercises

NATO training entities like the Joint Warfare Centre (JWC) in Stavanger and the Joint Force Training Centre (JFTC) in Bydgoszcz were established in October 2003 and March 2004, respectively. Since their



(ISR) roles in generally permissive environments, where adversaries did not possess credible air forces or counter-air capabilities.

The Russian invasion of the Crimean Peninsula in 2014, its support and involvement in Eastern Ukraine, as well as their involvement in the Syrian Conflict and in Libya, made Europe and North America aware that their primary focus on crisis management skills did not meet the need of allied forces and more generally of an Alliance whose core objective is to defend against any potential peer or near-peer aggressor. Developments in technology (e.g. artificial intelligence, high-speed and high-capacity data transfer) and re-armament efforts of Russia and other countries (including new long-range attack missiles, enhanced systems for Anti-Access/Area Denial [A2/AD], and hypervelocity weapons) provided a 'wake-up call' to

many NATO countries that the Alliance needed to re-invigorate its own vision of Collective Defence.

JAPCC's Support to Exercises

When JAPCC was established in 2005, its mission was to 'facilitate Joint Air Power Transformation', which included aspects ranging from 'concept development' to 'evaluation assistance and lessons learned activities'. The initial focus was to serve as a Think Tank for further development of Air and Space Power through drafting conceptual papers and providing contributions to NATO concepts and the development of Allied doctrine and doctrine-related documents. This work also included valuable contributions to training and exercises on a case-by-case basis. Starting in 2012, and underlined by a Letter of Agreement (LoA) with JWC,¹ the JAPCC formalized its support to exercises with an emphasis on the operational and strategic levels, i.e. the training of Joint HQs (Joint Force Command [JFC]-level) and components within Allied Command Operations. The impetus for this formal agreement was a lack of adequate specialist knowledge at the JWC, at the time, within the realm of Air and Space Power.





The LoA with JWC stipulated that the JAPCC would provide specialist knowledge and experience in Air and Space Power to assist in the delivery of training and exercise activities aimed at improving scenario development and providing trainer/observer teams, Exercise Control (EXCON) manning, and analysis at all stages. The common objective of both organizations was to provide, on a reliable basis, urgently needed expertise for agile and effective training of operational/strategic level audiences in order to meet the requirements of Collective Defence in future warfare environments. Not based on a formal agreement as with the JWC, but 'naturally' linked through common leadership,² the JAPCC soon provided its functional capabilities and subject matter expertise as well in support of Allied Air Command's (AIRCOM) annual exercise Ramstein Ambition (RAAM), thereby providing assistance to further development and refinement of Air Command and Control in NATO.

Realistic OPFOR Operating in Air, Space, and Cyberspace

The first exercise JAPCC supported under the LoA was Steadfast Jazz 13. An exercise conducted with a new scenario, named SKOLKAN, which focused on a limited NATO Article 5 scenario. Initially, when the JAPCC team arrived in Stavanger for the Main Events List/Main Injects List (MEL/MIL) scripting workshop, it was still unclear what role the team would play within EXCON. The desire was to keep JAPCC personnel together, as one team, to better highlight JAPCC as a supporting entity. Consequently, it was decided that JAPCC would take on the role of Red Air, or OPFOR Air. Unfortunately, JAPCC was not part of the SKOLKAN scenario development and was subsequently presented with pre-defined adversary air capabilities. The support delivered during this first exercise became crucial to the JWC/JAPCC relationship; because

it revealed that the scenario, as it had been developed so far, did not sufficiently reflect realistic and credible capabilities that were required to effectively train the audience. The JAPCC team also included a Space Subject Matter Expert (SME) in an attempt to introduce Space-related injects, but due to the late addition of JAPCC to the process the Training Audience (TA) was

with a multitude of other systems, such as coastal defence cruise missiles, an updated naval capability, and modern ISR capabilities. An overall more aggressive posture of OPFOR could finally be provided in support of the next major exercise, Trident Juncture 16 (TRJU16). The package aimed to replicate an A2/AD environment, which was duly challenging to the TA.



not adequately manned or prepared to deal with the Space aspects during that first exercise. It was therefore decided that the next iteration of the SKOLKAN scenario would have to include more up-to-date and realistic OPFOR Air capabilities. Despite the fact that the SKOLKAN scenario focused on limited operations, up to and including a Small Joint Operation (SJO) with a maximum of 300–400 air sorties per day, it provided a viable basis for further development.

Between 2013 and 2016, the JAPCC and the JWC further developed the scenario to a point where SKOLKAN's Air and Space capabilities were updated to reflect the most recent potential adversary capabilities, specifically in the field of Surface-Based Air Defence, modern aircraft types, (stand-off) weapons, jamming systems, Space-based systems, and anti-satellite systems. As a result, the scenario included multi-layered OPFOR Ground-Based Air Defence systems in combination

As a culmination of the SKOLKAN experience, having analysed the TA dilemmas and responses, JAPCC decided in 2016 to develop a briefing/training package to assist in accelerating the development of TAs skills. The briefing, entitled 'Component Integration Challenges in Combatting Advanced Layered Defence Systems (A2/AD)', not only analysed what A2/AD is and concepts on how to deal with it, but it also highlighted the ways various TAs had dealt with it in the past, including exercise adjudication from JWC and how an analysis of their results had been conducted. The initial briefings on current A2/AD structures and how exercises were replicating those systems were delivered at Supreme Headquarters Allied Powers Europe and JFC Brunssum. After being enthusiastically endorsed by the JWC Commander, word of what JAPCC was offering spread quickly. Since that initial briefing to NATO leaders, the JAPCC has presented the information at nearly 40 events, including Key Leader



Training events at both JFC Naples and Brunssum, air staffs in Romania, Italy, Germany, and to units in The Netherlands, Spain, and Belgium, to mention a few.

Training at Major Joint Operation Level

A potential conflict with a peer or near-peer competitor might evolve to a level quickly exceeding the scale of a SJO. To reflect this, starting in 2017, the OCCASUS scenario was developed to be used for the first time in the Trident Jupiter 18 exercise. This scenario aimed at enabling operations in a NATO Article 5 context at a Major Joint Operation (MJO) level. It included the latest developments, technologies, capabilities, and doctrine of potential adversaries and was designed to begin in the preliminary stages of a conflict, with an initial reaction of the NATO Response Force and a simultaneous build-up of a major force to counter the aggression. The development of the OCCASUS scenario provided the opportunity to add a host of new and different OPFOR capabilities from the Air, Space, and Cyberspace domains. As JAPCC had involved Space and Cyberspace SMEs in its exercise support since 2014, it was logical that these experts were included in the development phase of the scenario. As a result, significantly new and emerging capabilities were added, such as: OPFOR 5th generation fighters, air-launched hypersonic missiles, specialized jammers,

Low Earth Orbit satellites, Global Positioning System jammers, directed energy weapons and cyberspace warfare. Additionally, an offensive component of the A2/AD concept was introduced, namely deep-strikes into NATO territory, raising the realism of the exercises to a new level.

The aim of adding these new capabilities was to raise the level of complexity, challenge the TA to a level never before seen and increase NATO's level of ambition. The TA was severely challenged, and dilemmas were delivered up to and including the strategic level. Many of the new capabilities and tactics were unleashed from the first morning of the exercise, surprising and forcing the TA to adjust their plans right from the start. Throughout the subsequent days, reactions and decisions were sought up to the highest levels in the chains of command of every HQ involved.

Adaptations to Train the Air Component

Outside the JWC-led exercise arena, AIRCOM's main exercise, RAAM, continued to be developed with added layers of complexity and new Tactics, Techniques, and Procedures (TTPs). This was a gradual process that had to be managed carefully to keep the exercise at the Air operational level, primarily an Air Component's exercise. AIRCOM used the new, more

complex scenarios developed by JWC and further adapted them by offering additional opportunities to develop TTPs in a very dynamic air specific environment. This provided the perfect vehicle to expose the Air Component's TA to increasingly more complex dilemmas, including the Space and Cyberspace domains' aspects. One of the delivered events was a multifaceted cyber inject that culminated in a complex OPFOR Composite Air Operation (COMAO) which included false tracks, introduced via simulated malware, resulting in the COMAO appearing to be twice as large as it was in reality. Due to the innovative and imaginative challenges delivered to the TA, the RAAM19 exercise was considered by HQ AIRCOM to be one of the most successful and challenging exercises of the past ten years.

The Future of Exercise Support

What of the future for OPFOR (Air) support to exercises? It has become clear in recent years that the provision of a professional and specialized OPFOR is an essential part of delivering credible and effective training to NATO. It challenges the TA, using developing and imaginative concepts, which, in turn, forces innovation and creativity in training. This methodology will continue to be an effective tool, which can be further improved to assist in the development of new TTPs while staying in step with advances in technology or changes in adversary tactics. As the JAPCC OPFOR Air concept is becoming more successful and well known for delivering enhanced training, the requests for support from wider exercise audiences are constantly increasing. This in itself validates those initial efforts from the

humble beginnings eight years ago to the concept of a professional OPFOR, which is now an essential and effective part of present and future NATO training.

The future of warfare will likely see increasingly more complex operations across all domains; the term currently used to describe and summarize this scenario is Joint All-Domain Operations (JADO). It encompasses those actions taken by the joint forces of two or more nations, comprised of all available domains, integrated in planning and synchronized in execution, at a pace sufficient to effectively accomplish the mission.³ JADO will see an exponential increase in the traditional breadth and cross-domain harmony of decisions made, and actions taken, in a synchronized manner over an expansive and ever-changing battlespace. To enable the ability to consider all-domain effects and manoeuvre in and through all domains, it will require historic innovations in terms of training and education. The training and education plan will not only be innovative in and of itself, but the updating process of the curriculum and the flexibility of the training syllabus will require equally novel and evolving solutions. The future leadership, education and training plans will also need to incorporate these extremely challenging aspects of combined, joint all-domain warfare. The JAPCC remains committed to support the introduction of these aspects of modern warfare in exercise scenarios in the years to come. ●

1. Letter of Agreement between Joint Air Power Competence Centre and Joint Warfare Centre, 12 December 2012.
2. The Commander of Allied Air Command, headquartered at Ramstein Air Base, Germany, is also the Director of Joint Air Power Competence Centre at Kalkar, Germany.
3. NATO JADO: A Comprehensive Approach to Joint All-Domain Operations in a Combined Environment, JAPCC Leaflet, February 2021.



Lieutenant Colonel (ret.) Ed Wijninga

manned, from June 2013 until April 2021, the Education, Training, Exercises & Lessons Learned Section Head position at the JAPCC. Prior to this posting, he was the Branch Head Offensive and Support Operations at the Combined Air Operations Centre Uedem, Germany. Other positions include Staff Officer Close Air Support in the Netherlands Maritime Force at Naval Base Den Helder. He also served for two years as Operation Planner at the J5 section of the Directorate of Operations in the Ministry of Defence in The Hague.

During 2004/05 he attended the Joint Advanced Staff Officers Course at the Senior Staff College in The Hague and graduated with an Executive Master degree in Security and Defence (EMSD).

To Be or Not to Be Classified

Why Over-Classified Documents Make NATO's Life Harder: The Overarching Space Policy as a Prominent Example

By Lieutenant Colonel Tim Vasen, GE AF, German Air Force HQ

Introduction

Space Support plays a significant role in modern warfare and is a key enabler for NATO's technical advantage. Worldwide technical developments challenge this advantage, while Space has become congested and contested. Consequently, NATO developed an Overarching Space Policy (OSP)¹ in 2019, which finally led to the declaration of Space as an operational domain for NATO at the end of that year.² However, the OSP was classified at the NATO Restricted level and hence, is not available to the media, the public or potential adversaries.

Following Sun Tzu's famous quote **'Keep your friends close but your enemies closer'**, a publicly available version of the OSP would lead to increased understanding of Allies' intentions with regard to Space and Space-based capabilities. The decision to keep the OSP classified resulted in media speculation, not only by potential opponents, on the content of this policy.^{3,4} For this article, the OSP is used as a prominent example of the author's hypothesis. Most of the arguments used therein apply to other Space-related NATO documents as well.

(UN)CLASSIFIED



Why does NATO not continue its reform on strengthening transparency by applying it also to its Space Policy?

Transparency and Deterrence

Transparency and deterrence go hand in hand. It is reasonable to assume that the knowledge concerning potential counteractions, in case of a hostile act, leads to a more sober risk assessment on the side of the aggressor. Additionally, it creates an environment of greater trust between the public and the military/political establishment. NATO has done this in the past by making strategies publicly available, such as the Joint Air Power Strategy⁵ and the Allied Maritime Strategy.⁶

Dr Kestutis Paulauskas, a Senior Strategy Officer at NATO Allied Command Transformation and former member of the NATO International Staff, stated 'The credibility of deterrence – in either of its iterations – rests on a combination of 1) political resolve, 2) capability to inflict pain and 3) clear communication of said resolve and capability.'⁷ Judging OSP based on this definition, NATO is lacking at least two elements due to the classification and the non-public release of its OSP. The NATO Military Committee meeting, on 14 October 2019, pointed out the relevance of Space in NATO's defence and deterrence.⁸

Several NATO nations⁹ as well as the Russian Federation¹⁰ and the People's Republic of China (PRC)¹¹ have released transparent national Space policies. Neither the PRC nor the Russian Federation are role models for transparency but, due to the relevance of Space to their militaries and economies, they decided to go public with their plans. It is logical to assume that those are sanitized versions for public release. Full versions, for internal use, are presumed to contain parts covering critical information being, for this reason, likely classified.

Is the existence of a classified policy more deterring than a published one?

Classification Issues

There is a need to classify information the deeper it goes into critical planning processes. Documents of this type may include a classified information section, but that does not mean that the entire document has to be classified. NATO classification rules allow for such an apportionment in its policy documents.¹² This means that every defined part of a document, whether a paragraph, sentence, or chapter, can get the classification it needs, whilst the rest remains releasable to the public. This way NATO manages its data and information while avoiding over-classification. Structuring a document in this way requires a higher amount of work, because as each section has to be assessed and may have a different classification. However, this extra effort upfront will make the handling and use of the document much easier. Unfortunately, the referenced security guideline identifies this marking as mandatory only for documents classified as confidential or above. Compulsory regulation of documents classified as restricted or even unclassified is not included. The majority of the information in most NATO Unclassified or Restricted documents is publicly available or marked as releasable to the public, so the adaptation of the Allied Command Operations Security Directive to portion-mark documents with these classifications would make them much easier to handle and facilitate appropriate information sharing and interoperability.

Additionally, NATO personnel working with the content of Space policy need clear guidance on what can be publicly discussed and addressed. This is important when personnel contact other experts from industry, media, and the military who are not necessarily cleared for NATO classified documents. When information is over classified and unnecessarily restricted, this can significantly hinder effective collaboration and create scepticism in the minds of partners.

Is it worth saving time in the development phase of a document but lose more time, as well as transparency, in using after its release?



International Recognition and Responses

Acting diametrically opposed to previous transparent policies, classifying of a fundamental document such as the OSP invites speculation and potentially wilful misunderstanding by a potential adversary such as the Russian Federation or PRC. The Russian Federation's media quoted a Russian Foreign Ministry's official with a critical statement in response to the declaration of Space as an operational domain.¹³ Even when NATO Secretary General Jens Stoltenberg's statement on the declaration was included, it was still a weaker signal than having the chance to present a policy clarifying NATO's intentions in that domain. Other media reactions on NATO Space activities can be found at Al-Jazeera¹⁴ and the Global Times of China.¹⁵ These examples start speculation on activities and courses of action that could have indeed been prevented, or at least disproved, with a publicly available policy to present.

Shall NATO set itself up for this kind of media echo without having an available document to disprove misinformation?

Western Think Tank and Media Speculation

The non-profit information service NATO Watch, a critical but not strictly negatively-driven service, aims

at improving NATO transparency. In the case of the OSP, the principal critique is that even compared to the United States (US), which had made several national security policies open to the public, NATO does not follow suit. This keeps, by their assessment, the public out of the loop.¹⁶

The US news agency Consumer News and Business Channel released an article about the response and fear that the Russian Federation has with NATO activities to treat the Space domain as an operational domain and hence the 'militarization of space by NATO'. According to the western analysts quoted in the article, most of the fears and assumptions were caused by the lack of information and non-transparency due to the classification of the official source documents.¹⁷

Alexandra Stickings, a former Space Security researcher of the Royal United Service Institute, analyses the NATO steps in Space security and speculates about the invocation of Article 5 of the NATO treaty¹⁸ in case of an attack against a Space asset operated by one of its member nations.¹⁹ She states that due to the classified OSP, this topic is not yet clearly explained by the Alliance. A little more pointed are the complaints about the classified OSP made by Benjamin Silverstein, a research analyst at Carnegie Endowment for International Peace. According to him, the classified policy diminishes NATO's core security benefits, and



that lack of transparency on the question of whether and how NATO's Article 5 is applicable to Space is of major concern.²⁰

Most of the speculations deal with the topic of the invocation of Article 5 of the NATO treaty. Specifically, in the case of Space, where a potential attack will most likely occur outside of the geographical area defined in Article 6 of the NATO treaty. This can be compared to potential attacks in the Cyber domain, also a NATO operational domain. In this case, the NATO rules are clearly defined and transparent.²¹

Why is NATO not taking a more proactive approach to stopping these kinds of speculations and assessments on the OSP?

Assessment and Recommendation

NATO should maintain its credibility as a reliable and defensive Alliance that contributes to deterrence through transparency of its source documents. Particularly, in the information age, having official documents available to counter or disprove false or offensive critical statements that may cause further adverse discussions on media or social networks is a benefit. The way NATO approaches the Space topic, using official statements from the Secretary General,

is not as assertive as having a policy releasable to the public. Compared to the transparency in Space security provided by many western countries, as well as the Russian Federation and PRC, NATO's non-transparency leads to unwanted and unneeded speculations and assessments that would otherwise be easily avoided.

Using the classification guidelines more thoroughly and adopting them as mandatory at all classification levels will facilitate better dissemination of the relevant portions of the documents, once released. The 'easy', currently in use, way of just classifying the mentioned documents as a whole, leads to over-classification and inhibits cooperation.

Consequently, already existing documents such as the OSP should be reviewed and marked in line with the proposed classification guidelines.

Finally, it is recommended that NATO considers issuing a 'releasable to the public' version of the OSP to have a document available to mitigate or rebuff speculation and uninformed critical or false media reports.

That brings us back to Sun Tzu's quote to:

'Keep your friends close, but keep your [potential] enemies closer' ●



© yui/Shutterstock.com

1. NATO HQ (2019), NATO Defence Ministers approve new space policy, discuss readiness and mission in Afghanistan, https://www.nato.int/cps/en/natohq/news_167181.htm (accessed 23 March 2020).
2. NATO HQ (2019), Foreign Ministers take decision to adapt NATO, recognize space as an operational domain, https://www.nato.int/cps/en/natohq/news_171028.htm (accessed 23 March 2020).
3. TASS (2019), Russia to closely monitor NATO's activity in space, <https://tass.com/defense/1091577> (accessed 1 March 2021).
4. B. Silverstein (2020), NATO's return to Space, <https://warontherocks.com/2020/08/natos-return-to-space/> (accessed 11 February 2021).
5. NATO (2018), Joint Air Power Strategy, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180626_20180626-joint-air-power-strategy.pdf (accessed 4 March 2021).
6. NATO (2011), Allied Maritime Strategy, https://www.nato.int/cps/en/natohq/official_texts_75615.htm (accessed 4 March 2021).
7. Dr Kestutis Paulauskas, Space: NATO's latest frontier, <https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html> (accessed 1 March 2021).
8. NATO (2019), Space is essential to NATO's defence and deterrence, https://www.nato.int/cps/en/natohq/news_169643.htm (accessed 20 March 2021).
9. As examples, Space policies and Space related security documents of the US, Canada, France, Germany, Italy and Great Britain can be downloaded from official websites.
10. Russian Federation, approved by the President; Military Doctrine of the Russian Federation, Moscow, December 2014; President of the Russian Federation, Russian Federation National Security Strategy, Moscow, December 2015.
11. State Council of the People's Republic of China, White Paper on Space activities, 2016, http://english.www.gov.cn/archive/white_paper/2016/12/28/content_281475527159496.htm (accessed 24 August 2020); State Council Information Office of the People's Republic of China, China's National Defense in the New Era, 2019, translated version <https://www.andrewerickson.com/2019/07/full-text-of-defense-white-paper-chinas-national-defense-in-the-new-era-english-chinese-versions/> (accessed 2 September 2020).
12. NATO ACO (2019), ACO Security Directive, Brussels, Supreme Headquarters Allied Powers Europe, NATO unclassified, 28 January 2021.
13. TASS (2019), Russia to closely monitor NATO's activity in space, <https://tass.com/defense/1091577> (accessed 1 March 2021).
14. Al Jazeera (2019), NATO declares space an 'operational domain', <https://www.aljazeera.com/economy/2019/12/4/nato-declares-space-an-operational-domain> (accessed 26 February 2021).
15. Global Times of China (2020), NATO space center serves US military superiority, provokes space race, <https://www.globaltimes.cn/content/1204220.shtml> (accessed 4 March 2021).
16. I. Davis (2019), NATO's new Military Strategy and Space Policy: Why are parliamentarians and the public being kept out of the loop?, https://natowatch.org/sites/default/files/2019-06/nato_watch_observatory_no.50.pdf (accessed 4 March 2021).
17. H. Ellyatt (2019), Putin fears the US and NATO are militarizing space and Russia is right to worry, experts say, <https://www.cnn.com/2019/12/05/nato-in-space-putin-is-worried-about-the-militarization-of-space.html> (accessed 2 March 2021).
18. NATO (1949), The North Atlantic Treaty, https://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf (accessed 29 August 2019).
19. A. Stickings (2020), Space as an operational domain: What next for NATO?, <https://rusi.org/publication/rusi-newsbrief/space-operational-domain-what-next-nato> (accessed 5 March 2021).
20. B. Silverstein (2020), NATO's return to Space, <https://warontherocks.com/2020/08/natos-return-to-space/> (accessed 11 February 2021).
21. NATO (2019), NATO will defend itself, https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en (accessed 4 March 2021).

Lieutenant Colonel Tim Vasen DipEng, MSc

served for several years in commanding and staff positions within the artillery branch, including a deployment to KFOR as company commander of the DEU ISTAR-company before becoming a career intelligence officer. Serving 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). From October 2017 until August 2021 he was a member of JAPCC, responsible for Space Intelligence. In August 2021 he joined the German Air Force HQ, responsible for Space Intelligence development.





The TLP and the Pace of Change

TLP Challenges and Strategy

By Colonel Carlos Presa, PhD, SP AF, TLP

By Lieutenant Colonel Zachary Mellor, US AF, TLP

By Wing Commander Jonathan Millington, UK AF, TLP

Introduction

Change is associated in many cases with necessary actions, actions associated with positive effects, in politics, in aesthetics, in life. But this statement is not necessarily true if the changing subject already constitutes a relevant model of success. Altering the pillars and structures of a well-established working programme can inadvertently have unexpected negative impacts over some of its areas, and, for this reason, each change must be processed, analysed, and led through a sane and thoughtful decision-making process.

This is the exact issue with the Tactical Leadership Programme (TLP). TLP is overseen by a multinational headquarters based at Los Llanos Air Base, Albacete. It is composed of personnel from the 10 NATO member nations participating in the programme. Its main objective (Mission) is 'to increase the effectiveness of allied tactical air forces through the development of leadership skills, mission planning, briefing, tactical flying and debriefing skills, and doctrinal/conceptual initiatives'.¹

Throughout its 43-year history, TLP has become the focal point for NATO's allied air forces tactical training,

and the associated knowledge and leadership skills. Such skills are considered critical if NATO is to effectively face today's tactical air challenges. This has, is, and will continue to be achieved with the effort, dedication, and professionalism of yesterday's, today's, and tomorrow's TLP staff, a diverse and talented workforce.

TLP has navigated well through the different strategic, tactical, and technical stages of the last decades. The pattern of change has been based not only on the technological advances of modern systems, but also upon additional dynamic necessities such as the consolidation and growth of its members' mutual trust and willingness to operate together.

Operation Allied Force, International Security Assistance Force (ISAF) mission, Operation Unified Protector, and multiple air operations framed in diverse campaigns are a testament to how TLP graduates bring undisputable value to the Alliance or any international coalition when it comes to integrating Tactics, Techniques, and Procedures (TTPs), criteria, and effort. This is the product of a shared methodology, syllabus, and camaraderie that enables the plug & play effect that precisely represents one of the major defining characteristics of NATO air forces. Combined with technological superiority, all these facets are crucial in maintaining Alliance's strategic edge.

Absent from the implementation of an effective strategy, an accelerated change pattern may induce erratic decisions. A strategy is a plan comprised of interrelated actions to achieve a long-term goal. TLP has designed and is currently applying its own strategy to ensure that change increases the success of its leadership programme, which is fast approaching its 50th anniversary.

The TLP Strategy

The latest TLP strategy is based on its declared mission and was proposed and approved during the 2020 Steering Group (SG). The final objective of the strategy is twofold: to remain relevant with respect to the needs of its members whilst also aligning with the latest challenges and changes facing TLP. Such challenges,

which adjust the operational tempo with which TLP wishes to train, include technology, infrastructure, doctrine, participants, and, fundamentally, scenarios and opponents.

Likewise, the TLP strategy is based on several premises:

- The airspace enjoyed by the TLP, already established in the Aeronautical Information Publication Spain, is ideal for the activities planned to be carried out regarding size, weather, and allotted land and maritime portions.
- The integration of Future Combat Aircraft System projects to include connectivity.
- Systems procured by NATO nations will be at various stages of development.
- Budgetary constraints will continue.
- The core air power roles as defined in NATO's Allied Joint Publication 3.3 (B)² for Air and Space series will remain as a solid reference.
- Information and data sharing limitations, national security requirements, caveats, constraints, and boundaries will be present and will demand management in TLP-like forums.

Recognizing these preconditions, five Lines of Operation (LoO) have been developed. This will allow this strategy to be realized at an operational level, which is, to act on each area in a particular way, but also to coordinate inclusively as part of the whole strategy. These LoOs and their associated milestones correspond to the inferences of a deductive planning process, in other words, the things we can sequentially do to achieve our goals. All LoOs are interconnected, all converging towards the execution of TLP's mission and the realization of TLP's vision, which clearly states that TLP will remain aligned and relevant.

LoO 1: Integrating 4th and 5th Generation Aircraft Operations

Doctrinal initiatives at the NATO level, related to the integration of 4th and 5th generation platforms gravitate between several options. Some are provided through information integration solutions, which in turn have been merged by the on-board sensors.



Others are based on the reorganization of conventional Command and Control (C2) structures, which in some tactical contexts may consider 5th generation aircraft as a C2 sub-node. The distribution and orchestration of platforms from dissimilar generations, manned or not, is one of the challenges faced by the TLP, which represents at the tactical level the perfect Live, Virtual, Constructive and Live-Virtual laboratory for the Alliance to consolidate this integration process in a multinational context.

The current decade represents a period of transition in which the initial coexistence of 4th and 5th generation platforms will continue to expand. At the national level, some nations will continue to design interim processes in which 5th generation assets will replace the 4th generation ones. TLP will enhance the level of instruction provided to their mission leaders, helping to bridge the gaps between the training requirements of these two generations and contributing to the avoidance of potential fractures within these two training communities. Furthermore, through its various syllabi, particularly through opportunities that will

open up in terms of virtual and live-virtual training, TLP will represent an unbeatable and optimal opportunity to aid nations in their transition to the newest generation of aircraft.

Soon after the inspection and evaluation carried out by the United States Air Force (USAF) in 2019, Albacete Air Base was certified for the operation of 5th generation aircraft. At present, the milestones (decisive conditions) included in this LoO refer mainly to infrastructure, such as the provision of a Deployable Debriefing Facility (DDF) farm with the required physical security elements. The DDFs will be distributed throughout TLP's infrastructure to enhance the regular and safe operation of 4th and 5th generation multi-aircraft detachments.

Likewise, work is being done on installing an approach radar in the Albacete Air Base to speed up the recovery phase of missions involving large numbers of aircraft, thus enhancing flight safety. This Airport Surveillance Radar service entry is expected to happen in 2022.

LoO 2: Agile Combat Employment (ACE)

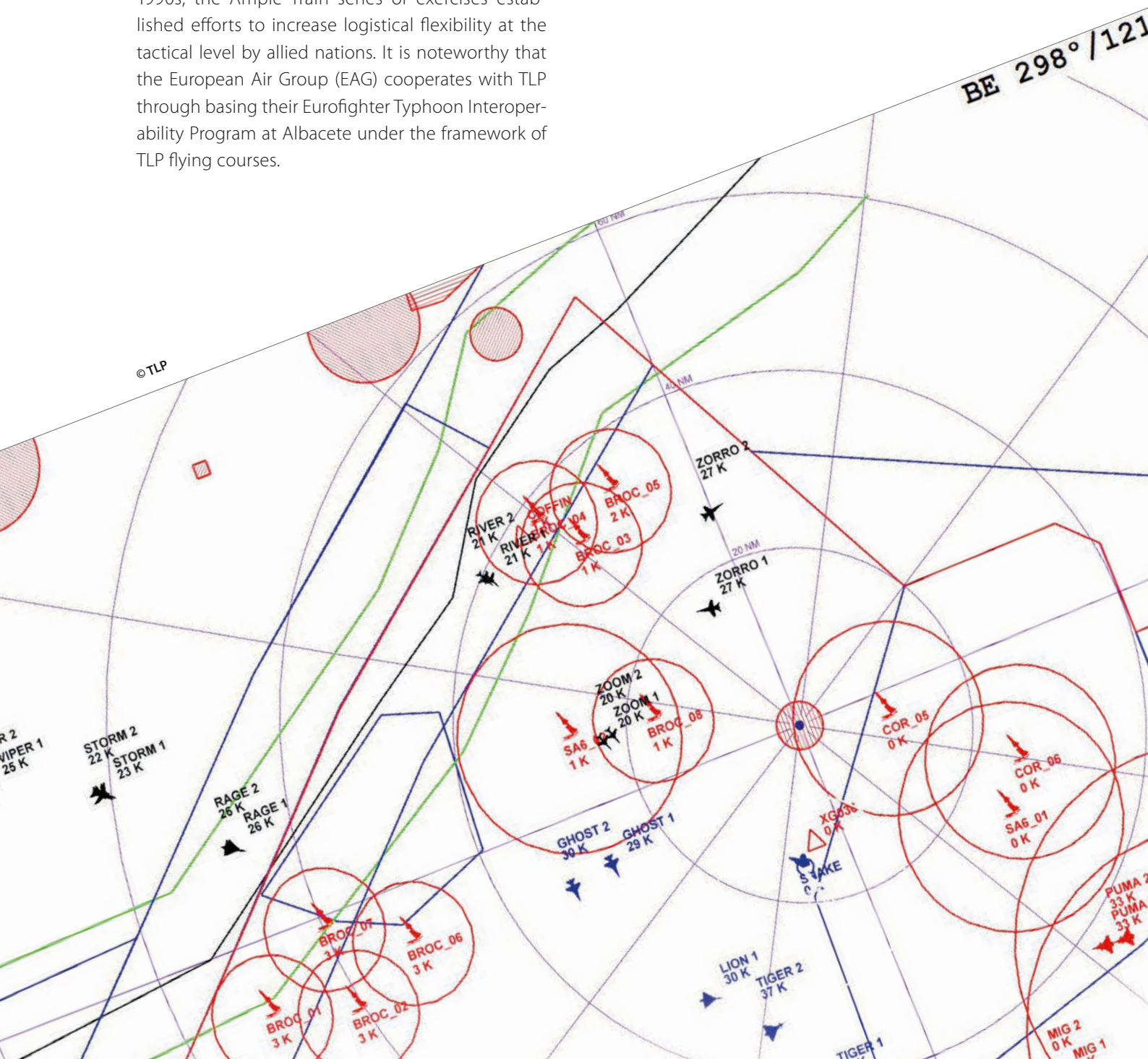
The USAF defines ACE³ as a 'proactive and reactive operational scheme of manoeuvre executed within threat timelines to increase survivability while generating combat power'. TLP scenarios will incorporate those ACE characteristics that the fighting air assets can employ to protect personnel, equipment, and facilities before, during, and after an attack. Thus, they will continue generating combat power from locations other than their Main Operating Bases.

Concepts related to ACE have been addressed and practiced in other formats and forums. Since the 1990s, the Ample Train series of exercises established efforts to increase logistical flexibility at the tactical level by allied nations. It is noteworthy that the European Air Group (EAG) cooperates with TLP through basing their Eurofighter Typhoon Interoperability Program at Albacete under the framework of TLP flying courses.

Including ACE as a LoO fosters an agile combat culture among the participants. A first step is to include the ACE concept in the supporting academic courses, followed, as a second step, by the introduction of ACE-related injects and maintenance cross-servicing practices within the flight courses.

LoO 3: Virtual and Live-Virtual Training

This LoO is the most transformational and addresses all the changes that will be introduced with the use of a new tool: the TLP flight simulator.



This simulator consists of more than 30 fighter cockpits and Ground Control Interception positions so that virtual pilots and controllers can all carry out training whilst seated in the same room. It also includes modes related to the 5th generation aircraft and a huge array of options for modelling platforms, threats, and weapons.

The TLP Simulator, being a laboratory for complex tactical air missions, will allow the processing and defining of a multitude of new possibilities directly relating to and replicating the integration of all types of systems that are actually playing in Virtual and mixed Live-Virtual environments.

Tactical synergies detected in the real world can be later modelled in the virtual world and reciprocally, be it the cooperative interaction between different platforms, weapons, sensors, and air power roles, as well as among other capabilities that are currently introduced such as Miniature Air-Launched Decoys, electro-magnetic pulse weaponry, Tomahawk Land Attack Missile type weapons, as well as others.

Virtual maritime and land power platforms may be introduced to enrich the tactical context of the Blue (friendly) Forces. Likewise, both the TLP and the participating nations will be able to use the simulator to model and execute wargaming of specific missions or scenarios.

This new simulator incorporates connectivity with C2 systems to provide certain degrees of Live-Virtual training. It will be the alternate tool to be used in case of bad weather or other limiting factors. Also, it is already possible to fly virtual Blue and Red (enemy) tracks, inserted into live-flying scenarios from the simulator's cockpits through the Link-16 network. The first Live-Virtual event (real Blue

fighters plus virtual Blue fighters versus virtually-generated tracks, both airborne and ground-based) took place in June 2021. TLP, in coordination with the Host Nation (HN) (operator of the C2 system and responsible for airspace management), will determine the levels of ambition that allow both the safe operation of the systems and optimal training.

Once simulator's capabilities are properly analysed, TLP's syllabi will be reviewed in order to propose new options to its SG. These options will mostly be a product of combining or mixing Live and Virtual training.

LoO 4: Contested Degraded Operations

The TLP deploys live ground and air threats during its flying courses. Many other regional stakeholders, like the European Defence Agency and EAG, are looking for mid-term solutions regarding a Red Air provision.

Live Red Air is provided by the different participating countries in accordance with TLP's Plan of Operations, while Live-Virtual Red Air can now be fed by virtual traces operated in real time either from the new TLP simulator or from future simulation facilities, which may become integrated into the HN's C2 system.

Regarding Red Surface-Based Air Defence (SBAD), the TLP simulator's intelligence generator is the perfect tool to introduce complex orders of battle, including proper opposing forces with SBAD settings based on patterns of movement and Emissions Control procedures. Simulation of enemy SBAD at an appropriate information classification level (TLP has just incorporated a NATO Secret Wide Area Network, thus the simulator supports classified information) will permit the reconstruction in the virtual environment of specific tactics observed in various scenarios, particularly those typical of Anti Access-Area Denial scenarios. The incorporation of a wideband joint threat emitter, planned for the year 2022, will radically improve the quality of such tactical contexts.

TLP and the HN have supported various site surveys from the participating nations to identify possible unpaved landing strips that can be used in missions that



require them (like Slow Mover or Personnel Recovery). These types of operations enrich the scenarios that already include emitters, inflatable decoys, and other supporting live Ground-Based Air Defence elements (NASAMS, PATRIOT, CROTALE, MISTRAL).

LoO 5: Joint All-Domain

Air combat platforms will network together and be orchestrated with other land and maritime platforms while executing complex missions. The cyber domain will provide transversal connectivity features between domains and/or components, resulting in complementary C2 architectures parallel to those of each component command.

TLP's cooperation with JAPCC is aimed at introducing relevant Cyber & Space aspects affecting the planning and execution of 4th & 5th generation Composite Air Operations (COMAO), as well as upgrading the joint portion of TLP's tactical scenarios by embedding JAPCC's lessons learned from its participation in the Trident Juncture computer-assisted exercise series.

It should be noted that this level of complexity may not have proper replication during the standard execution of the Flying or COMAO Courses, as the TLP Mission states that the main goal is to increase the effectiveness of the Allied Air Forces. Consequently, a Joint All-Domain Operations (JADO) overload may obscure this clear air mission. Furthermore, manning constraints are a limiting factor, as TLP instructors focus on the aforementioned air-centric tactical mission. Therefore, extra manpower would definitely be a significant asset to enhance this JADO step. However, once the TLP simulator is ready to take a step beyond regarding joint scenarios, it could offer TLP participants an air-centric introduction into the joint battlespace, which students may encounter in the future, while operating within the Air Component Command and in synchronization with other joint assets.

TLP in the Future

The TLP vision demands that it remain aligned and relevant. Throughout its history, TLP has successfully adapted to meet strategic, tactical, and technical transformations to effectively train NATO's allied air

forces to meet pertinent and exacting challenges. To continue to successfully navigate this path, and based upon the declared mission of TLP, these five intricately linked LoOs will ensure that TLP continues to achieve its long-term aim. ●

1. TLP Memorandum of Understanding, Section 1, 1. (2009), p. 7.
2. NATO Standard AJP 3.3, Allied Joint Doctrine for Air and Space Operations, Edition B, Version 1, published by NATO Standardization Office (2016), p. 1.8–1.17.
3. US Air Forces in Europe & Air Forces Africa, F-15s, F-16 and C-130s arrive in Poland for an Agile Combat Employment exercise, press release no. 010421, <https://www.usafe.af.mil/News/Press-Releases/Article/2576858/f-15s-f-16s-and-c-130s-arrive-in-poland-for-an-agile-combat-employment-exercise/> (accessed 3 June 2021).

Colonel Carlos Presa

is currently the TLP Commandant, being commissioned through the Spanish Air Force Academy as an officer in 1992. Following operational and instructional postings in several units, flying mainly the F-18 Hornet, he completed his command tour as the 462 SQN Commander in the Canary Islands. After graduating from the Joint Staff College in Madrid, he was posted as an Air-to-Air instructor at the Tactical Leadership Programme. Among other missions, he joined ISAF as the acting Air Liaison Officer, TACP Commander and Airfield Coordinator for the Spanish Battalion. He returned to the Staff College as an instructor in 2012, while from 2014 to 2017 was the Manned Air Defence SME at JAPCC. Colonel Presa holds a PhD in Linguistics and worked as a Professor at Universidad Complutense, Madrid.



Lieutenant Colonel Zachary Mellor

is the current TLP Chief Flying Branch, being commissioned through ROTC in 2003. As an F-15E Weapon Systems Officer at Seymour Johnson Air Force Base, he deployed in 2007 and 2009 to Afghanistan in support of Operation Enduring Freedom. Next, he served in the 391st Fighter Squadron, Mountain Home Air Force Base, Idaho as the Chief Security Manager and Flight Commander from where he deployed in support of Operation Enduring Freedom, Horn of Africa and a Theater Security Package, United Arab Emirates. Following that assignment, he continued flying the F-15E at Seymour Johnson AFB as a Formal Training Unit Instructor. Prior to his current position, he served in the Combined Air Operations Center at Torrejon Air Base, Spain.



Wing Commander Jonathan Millington

was commissioned into the RAF in 1986 and has completed three operational tours on the Tornado F3. A graduate of the UK Aerosystems Course he has completed trials management tours on the FA2 Sea Harrier, Typhoon, and various UAS platforms, including a tour as a UAS Requirements Manager, gaining a PG Diploma in Defence Acquisition Management. In 2012 he was posted to the US to hold the position of AWC F-35 SNR, where he maintained assurance oversight of all UK initial F-35 flying operations and engineer maintenance training, including responsibility for the establishment of the UK's F-35 mission-data reprogramming capability. Prior to TLP, he served in HQ SACT performing policy, concept, doctrine, and analysis including the development of NATO's Joint Air Power Strategy.



Joint Air and Space Power Conference 2021

Delivering NATO Air and Space Power at the Speed of Relevance

The JAPCC's Director, General Jeffrey Harrigan, had the honour to welcome 300 leaders and senior experts from Industry, Academia, and Defence, despite the challenges of the ongoing pandemic. They met from 7 to 9 September 2021 at the JAPCC's annual conference in the Congress Centre in Essen, Germany to discuss imminent and foreseeable challenges to NATO Air and Space Power. Among the distinguished delegates were three keynote speakers, Assistant Secretary General for Defence Investment, Mr Camille Grand, the Supreme Allied Commander Europe, General Tod D. Wolters, and the US Chief of Space Operations, General John W. Raymond and more than 20 panellists that offered their insights and perspectives.

The JAPCC conference took place at a time when NATO was about to start discussions on developing an updated version of the Alliance's Political Guidance, which provides the framework for the coordinated planning of an effective set of forces and is supposed to be published in early 2023. Therefore, the conference theme referred to a term, Speed of Relevance, that has also been used in some prominent US and NATO strategy papers to describe the need for enhanced and sped-up delivery of capabilities for defence.

Discussions at the conference provided various perspectives on how to ensure the 'Speed of Relevance' today and in view of possible crisis and conflict scenarios. What we perceive today as strategic competition needs to be understood in its full complexity and requires distinct answers. NATO nations will need to

invest in capabilities that continue providing for credible deterrence and defence.

Along with the traditional Land, Air, and Maritime domains, Cyberspace, the Electromagnetic Environment, and the Space domain will need to be further thought through and developed conceptually and doctrinally. We will have to make use of advanced technologies like Artificial Intelligence and the management of Big Data to provide for fully integrated and seamless sharing of information to enable superior cycles of planning, decision, and execution of joint operations across domains. A NATO-wide architecture with an aspirational design could be a basis to offer options for decentralization of both C2 and execution. This will require changing some deep-rooted habits, if not a cultural change.

We are thankful to our keynote speakers and panellists for their splendid contributions and the invaluable thoughts and perspectives provided, as well as to all our participants for the fantastic insights they shared with us. Moreover, the event's success would not have been possible without the tremendous support of our sponsors; we thank you all and look forward to seeing you again in 2022.

Finally, next year's Joint Air and Space Power Conference will further explore the complexities of ongoing global competition, the need for deterrence and defence, and debate those aspects that support Enhancing NATO Air and Space Power in an Age of Global Competition. Do not miss this excellent opportunity and save the date in your calendar now! ●





JAPCC Hosts 8th Annual Joint Air and Space Power Network Meeting

NATO and European Air and Space Future Challenges

On 17 November 21, the JAPCC hosted the 8th annual Joint Air and Space Power Network Meeting (JASPN) in Kalkar, Germany. In compliance with strict anti-pandemic measures, the meeting was organized as a one-day in-presence conference. To hold the meeting in person was a great opportunity and highly appreciated by all attendees and included representatives from NATO HQ International Staff, HQ Allied Air Command, NATO Science and Technology Organization, NATO Support and Procurement Agency, European Air Transport Command, European Defence Agency, European Air Group, Competence Centre for Surface-Based Air and Missile Defence, Integrated Air and Missile Defence Centre of Excellence, Command and Control Centre of Excellence, and Air Operations Centre of Excellence.

The JASPN is considered to be a most productive working opportunity and serves to foster collaboration and enhance synergy within the Air and Space Power community since 2014. It brings together international organizations that provide expertise in

the Air and Space domains to share thoughts and perspectives and identify areas of common interest and work to achieve efficient approaches while avoiding unnecessary duplication. This helps all organizations pursue efforts to collectively identify potential solutions in dealing with imminent Air and Space Power challenges.

Once again, this year's meeting proved to be an effective session with all twelve representatives presenting their organization's programme of work and focusing on those projects where the potential for mutual co-operation exists. As an event summary, a collaboration matrix was created to document and share identified projects, mutual interests, and lines of effort.

In the light of upcoming challenges and opportunities facing the Air and Space domains such as interoperability, resilience, and emerging technologies, the topics most discussed among the JASPN participants were in the realm of Joint All-Domain Operations/ Multi-Domain Operations (JADO/MDO). ●

JAPCC Hosts the NATO Air Operations Working Group

The 51st Air Operations Working Group (AOWG) 'hybrid meeting' was hosted by the Joint Air Power Competence Centre in Kalkar, Germany, from 26 to 27 October 2021. The meeting, chaired by the JAPCC Assistant Director Air Commodore Herber, brought together 16 participants (seven of which were virtual attendees) from 12 NATO nations and five NATO agencies.

During the meeting, 53 topics were covered with a specific focus on ensuring the effectiveness and interoperability of NATO forces engaged in air and space operations. Major items discussed included liaison reports from 19 agencies whose work is pertinent to the AOWG and the review of 15 Standardization

Agreements (STANAGs). The group also re-examined nine previously submitted terms to the NATO Terminology Office (NTO) and conducted a final assessment of the AOWG Terms of Reference receiving briefings from the Senior Air Information Exchange Panel (SAIERP), Allied Command Transformation (ACT), and the Joint Capability Group for UAS (JCGUAS). Finally, working group initiatives proposed to expand the AOWG's ability to gather and communicate current issues to the Military Committee Air Standardization Board (MCASB).

The 52nd AOWG meeting is expected to take place in Athens, Greece, in May 2022. ●

2021 Maritime Air Coordination Conference

On 5 October 2021, 24 delegates from nine nations, two NATO Commands, two COEs and eight national organizations gathered at the JAPCC for the annual Maritime Air Coordination Conference (MACC). The event was co-chaired by the JAPCC Assistant Director, Air Commodore Paul Herber, who represented ACT, and Rear Admiral Hans-Jörg Detlefsen, Commander Maritime Air NATO, representing ACO; this being the first meeting since 2019.

The MACC's overall aim is to promote the development of Maritime Air through focused discussion and debate. The theme of this edition was 'Carrier Strike Group – C2 within NATO'. The agenda focused on the growing MARCOM ambition to improve Carrier Strike Group (CSG) interactions and support to DDA STRATCOM opportunities, including CSG contributions to playbook activities.

Maritime Air representatives described the current CSG liaison work conducted by MARCOM with the UK, US, France and STRIKEFORNATO (SFN), as well as assisting in the preparatory activities for UK NRF22. Various discussion points from the MARCOM/SFN symposium, hosted in Northwood in September 2021, were briefed including opportunities to support future working practices by a shared approach to a Guide SOP for CSGs working with NATO. Representatives from the French and UK navies briefed their national CSG capabilities, organizations and processes, and their support to NATO. JAPCC presented one of its newest projects, NATO Joint All-Domain Operations (JADO), describing the aim and scope, study topics and work strands, and commonalities with the NATO Warfighting Capstone Concept. The next MACC is planned to be held in Northwood, UK in 2022. ●



Handover Ceremony of the Assistant Director Post in JAPCC

A New Era with New Challenges!

The handover ceremony marking the departure of Brigadier General Giuseppe Sgamba and the arrival of Air Commodore Paul Herber took place on Friday, 17th September 2021.

The ceremony was attended by prominent and high-ranking guests, marking the official handover of duties and responsibilities under the auspices of the JAPCC Executive Director Lieutenant General Klaus Habersetzer.

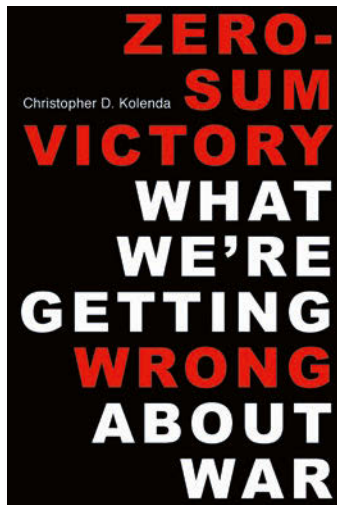
Air Commodore Herber, in his new function as the JAPCC Assistant Director (AD), thanked all attending the ceremony, complimented the outgoing AD for his successful tenure, expressed his appreciation of JAPCC's staff work and accomplishments, and conveyed his trust for a continued high level of performance in the future.

From the outset, Air Commodore Herber took charge of shaping JAPCC's activity by indicating his priority to ensure the relevance of JAPCC's work while fostering a professional, productive, and rewarding working environment.

Air Commodore Herber had the privilege of holding a plethora of leading positions, including Chief of Staff at Volkel Air Force Base, Chief of Staff at the Netherlands Defence Academy, Chief of Staff CFO at the Ministry of Defence, Commander of the Netherlands Defence Security Organization, and the Netherlands Defence Attaché to the United States of America at the Embassy of the Kingdom of the Netherlands in Washington, D.C.

The JAPCC will continue to evolve and adapt throughout its existence to remain further effective and relevant transforming Joint Air and Space Power. ●

‘Zero-Sum Victory’



By Christopher D. Kolenda;
The University Press of Kentucky;
October 2021

Reviewed by: Lt Col Henry Heren,
US Space Force, US Joint Staff J-5

As Western Powers strive to adapt to a world enmeshed in great power competition, with the lines blurred between peace, crisis, and conflict, they must strive to not only comprehend the methods but also the goals. Military planners and political leaders must become more nuanced in their approaches and can no longer default to ‘decisive victory – a vague and dangerous belief that the expert application of military power will force an adversary to capitulate’ (p. 9).

Christopher Kolenda’s *Zero-Sum Victory* explores the contemporary history of US military campaigns to demonstrate policy shortfalls with regards to war termination criteria. These recent experiences serve as prime examples for setting realistic political and military objectives prior to entering a conflict, as well as the difficulties which might be encountered trying to adjust to a poorly developed framework once the fight has begun.

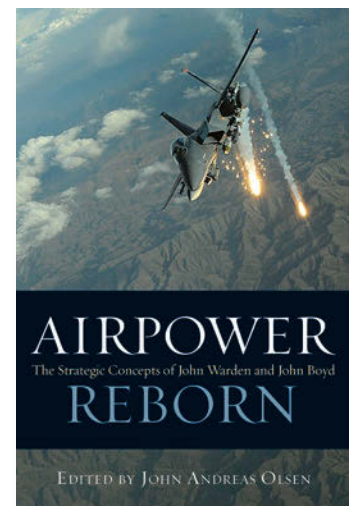
Military planners must develop an understanding ‘of the political and diplomatic dimensions of national power’, and appreciate that ‘outcomes broader than decisive victory can help policy- and strategy-makers develop a more realistic array of options’, (p. 257) and this book greatly assists in that effort. ●

‘Airpower Reborn’

Airpower Reborn reflects on the role of air power after the operations in Libya and Afghanistan. Edited by John Olsen, an academic with military expertise, the collection includes a philosophical and systematic approach to give a new vision for the air domain. It represents a compendium of five chapters composed of original works by authors which give different perspectives on the importance of air power. The writing follows a socio-philosophical style.

Starting from the first air doctrines and the Kuhnian concepts of ‘paradigm shift’, the book highlights the historical struggles of the independent air power inside traditional military doctrine. The theoretical approach is influenced by human history and found the roots in classic era – the Roman Empire and Renaissance (Machiavelli) – up to ‘scientific’ models of the 1900s (i.e., Douhet, Mitchell, Trenchard). The concept of Orient Observe Decide Act (OODA-loop) is the point of reference for analysing the adversaries, underlining the influence of the moral, manoeuvre and attraction. Boyd and Warden are still taken as the central point for building the projection of the air domain in the future.

The paradigm of independent air power appears the key point of discussions and represents a revised approach to revitalize the role of air domain in post-modern warfare. This book remains a Western-centric reviewing of air power in a world in which new technologies are leveraging the military-strategic vision. ●



By John Andreas Olsen;
Naval Institute Press Annapolis,
Maryland (US); 2015

Reviewed by: Maj Giuseppe Valentino,
IT AF, JAPCC

Air & Space Power Conference

20
22



Enhancing NATO Air and Space Power in an Age of Global Competition

11–13 October 2022
Congress Centre Essen, Germany



Save the date in your calendar:
www.japcc.org/conference

**Joint Air Power
Competence Centre**

snc[®]



INNOVATION. PERFORMANCE. AGILITY.

SOLVING COMPLEX CHALLENGES WITH
CUTTING-EDGE, MULTI-DOMAIN SYSTEMS
& EMERGING TECHNOLOGIES.

sncorp.com

